UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

CONSUMER ELECTRONIC PAYMENTS TASK FORCE

PUBLIC MEETING ON THE PRIVACY AND SECURITY OF ELECTRONIC PAYMENTS INFORMATION

Thursday, July 17, 1997

Federal Trade Commission

6th and Pennsylvania Avenue, N.W.

Washington, D.C. 20580

FEDERAL TRADE COMMISSION

I N D E X

CONSUMER ELECTRONIC PAYMENTS TASK FORCE REPRESENTATIVES:

Eugene Ludwig, Comptroller of the Currency
Consumer Electronic Payments Task Force Chairman

Robert Pitofsky, Chairman, Federal Trade Commission

Edward W. Kelley, Jr., Member, Board of Governors of the Federal Reserve System

Russell D. Morris, Commissioner, Financial Management Service

Jack Guynn, President, Federal Reserve Bank of Atlanta

Carolyn Buck, Chief Counsel, Office of Thrift Supervision, on behalf of Director Retsinas

Robert Russell, Director, Office of Policy Development, Federal Deposit Insurance Corporation, on behalf of Acting Chairman Hove

PANEL ON PRIVACY ISSUES

Demonstration:

David Chaum, Founder and Chief Technology Officer, DigiCash

Panelists:

Mary J. Culnan, Commissioner, President's Commission on Critical Infrastructure Protection

Susan Grant, Vice President for Public Policy, National Consumers League

Pamela J. Johnson, Counselor to the Director, Department of Treasury, Financial Crimes Enforcement Network (FinCEN)

Janet Koehler, Senior Manager, AT&T Universal Card Services, on behalf of Smart Card Forum

Deirdre K. Mulligan, Staff Counsel, Center for Democracy and Technology

Marc Rotenberg, Director, Electronic Privacy Information Center

Marcia Z. Sullivan, Director of Government Relations, Consumer Bankers Association

P R O C E E D I N G S

- - - - -

MR. LUDWIG: I'm pleased to welcome you to the second public meeting of the Consumer Electronic Payments Task Force. The emergence of the new electronic money products, like on-line and off-line, Stored Value Cards, Smart Cards, and Internet payments, has generated considerable public interest and even more concern about consumer issues, since these products generally are not subject to the same regulatory regime or industry standards that apply to more familiar payment mechanisms like credit/debit cards.

The Consumer Electronics Payment Task Force was established by Treasury Secretary Ruben to focus on this important dimension of development of new electronic money and payment technologies; that is, what is and will be the effect on consumers of these products. The mission of the task force is to identify consumer issues raised by electronic money, evaluate the extent to which these issues are being addressed by laws or industry practices, and identify innovative nonregulatory responses that may be needed for consumers in this developing market.

Consumers are most likely to benefit from, and use,E-money products if they understand the risks and benefits of the new products and if they know that their interests have been considered and addressed by the industry.

This consumer dimension is really important for not only the well-being of the consumer which is certainly critical, but also for the healthy development of this industry.

Among the issues of great importance to consumers are privacy and security. We have gathered a distinguished group of experts here today to discuss the privacy and security issues that may arise for consumers when they use these products.

In examining of consumer issues and concerns raised by emerging electronic payment products, the Task Force is especially interested in hearing from the public, and will carefully evaluate their views.

I can't stress this enough. We have held two public hearings, this being the second, and several informal sessions. We welcome written testimony, and other public expressions of interest in this issue.

Someone, I think it was Bill Gates, recently said that there is a tendency for people to be disappointed that a new technology doesn't develop in the first year or two and then a failure to appreciate how significantly the impact of that technology will be over a period of five-plus years.

And in this area I am persuaded that even if we don't have everyone using Smart Cards in the next year or so we are going to see a future where these products are going to be aggressively used. It's important to consider the consumer, primarily with

respect to these products.

Now, I'd like to introduce the representatives of the Task Force that are here today. I know that for each of them, the issues that are addressed by this Task Force are of paramount importance to them. We have worked well together.

Jack Guynn is President of the Federal Reserve Bank of Atlanta. Russ Morris is Commissioner of Financial Management Service. Governor Edward W. Kelley, known to most of you as Mike Kelley, is the Governor of the Federal Reserve System.

Robert Pitofsky is Chairman of the Federal Trade Commission and our real host today. Bob Russell, of the Federal Deposit Insurance Corporation, is sitting in for Chairman Skip Hove who had to testify this morning.

Carolyn Buck is Chief Counsel to the Office of Thrift Supervision and is here on behalf of Director Retsinas, who is also testifying today.

I also have to testify after this hearing and so may be called out. Bob Pitofsky has graciously agreed to chair the rest of this hearing. And without further ado let me turn this over to Chairman Pitofsky and others for any remarks they'd like to share before we begin.

CHAIRMAN PITOFSKY: On behalf of the Commission I'm delighted, to host this session of the Electronic Payments Task Force. As many of you know, indeed some of the witnesses today testified here in our hearings a month ago.

We held four days of hearings on privacy in the on-line marketplace. They generated tremendous interest and enthusiasm. And we all learned a lot from the hearings, and I look forward to a similar educational experience here today.

And I look forward to working with the Task Force. I still believe that self-regulation, industry self-regulation is the way to start in this area. And I hope we can make some progress in that direction.

MR. LUDWIG: Now let me introduce our panelists.

David Chaum is Founder and Chief Technology Officer for DigiCash. Mary Culnan is a Commissioner on the President's Commission on Critical Infrastructure Protection.

Susan Grant is Vice President for Public Policy of the National Consumers League. Pam Johnson is Counsel to the Director of the Department of Treasury's Financial Crimes Enforcement Network.

Janet Koehler is here on behalf of the Smart Card Forum. Deirdre Mulligan is Staff Counsel for the Center for Democracy and Technology. Marc Rotenberg is Director for the Electronic Privacy Information Center. And Marcia Sullivan is Director of Government Relations for the Consumers Bankers Association.

MR. CHAUM: Good morning, Mr. Chairman, and members of the Task Force. As an American pioneer in the new technology for privacy and a representative of a leading electronic commerce company, I'm very pleased to be here.

I think we can all agree that electronic commerce holds enormous potential. Also that privacy concerns for many Americans, as surveys have indicated, are a major impediment to realizing this opportunity. Thus, a solution could bring great advantage.

New technology for interaction privacy is proving to be such a solution. I'll be defining interaction privacy first by establishing its place within the set of related policy issues and then by showing its position in the spectrum of privacy issues by real systems, focusing on the key area of payments.

Next I will present examples of interaction privacy technology in commercial use for making payments on the Internet and demonstrate it briefly. And finally I will show you how this technology can be applied to the whole range of consumer payments and some general implications.

Three major policy issues relate to interaction privacy. The first is consumer protection. The U.S. led the world with its Privacy Protection Study Commission report 20 years ago this month. Its recommendations have a distinct consumer protection orientation.

The second issue is human rights. Those human rights that pertain specifically to the informational sphere I have called informational rights since 1985. As people become aware of the reality of purely informational dangers, and that protections are available, with history as a guide they will regard such protections as desirable and as human rights.

The third policy issue is that of beneficially shared resources generally referred to as commons. Examples are environmental concerns and free bandwidth that is the basis for the emergence as well as the character of the Internet.

To see how the three issues differ, consider a problem linked to each. Protection against false claims of privacy protection (which I will be coming back to), the use of encryptions and the right to keep one's own notes and records confidential, and the availability of essentially free bandwidth responsible for the Internet.

And to see how the issues overlap partly, consider an example problem for each pair. Encryption of messages to ensure their confidentiality when sent over networks allows people to combine into groups any informational commons and clearly intersects with informational rights.

Similarly junk mail and more general push technology fall within the consumer protection, but also are potentially the problem of pollution of a commons. I will discuss the importance of whose hardware platform consumers use later as both consumer protection and prevention of false incrimination aspects.

For the informational part of each policy issue to be meaningful, access to cyberspace must be available. At the core of the intersection of the three issues, however, and tied to some of our most cherished national values is interaction

privacy.

Interaction privacy is a term I have not used before today. I propose to define it as follows: The protection of individually identifiable data arising from interaction between individuals and organizations.

The term, organizations, is used broadly to mean commercial enterprises, public sector organizations, and even informal groupings of individuals. For instance, interaction privacy protects all of the data about who you telephone. To the extent that payments are implemented electronically, all the details of when, where, and the price of everything you buy, and everything you may do on the Internet including participating in discussions, polling, and some day even secrecy of your ballots.

Such protection is essential to democracy as it allows people to participate freely without fear of retribution. As cyberspace grows, interaction privacy becomes essential to the emerging digital agora.

Payments, however, play key roles since the cost of low-value electronic transaction continues to drop they are rapidly finding their way into many parts of our lives. Such transactions are pay T.V., phone cards, public transportation, load pricing, and as a pay-as-you-go model on the Internet.

If payment does not provide interaction privacy, then the growing range of things that themselves involve payments will be prevented from providing interaction privacy.

The privacy of information systems generally, but specifically consumer payments, can be seen as a spectrum from the no privacy at all to organization-controlled privacy to false privacy, which is a major danger, and finally to consumer-controlled or true interaction privacy.

The other dimension, technology ranges from paper-based to fully digital. One traditional approach of payments, so-called transfer orders like checks and credit cards, offer organization-controlled privacy at best. The organizations operating under the system can see the payor and the payee of each transaction.

Naturally, if the organization makes the payments public, there is no privacy. Organizations may even claim that they don't misuse or leak information, but of course you can never be sure. Plenty of examples of violations have come to light with various degrees of involvement of organizations who have access to data.

The really dangerous and disturbing category I have called false privacy is in fact organization-controlled privacy where consumers are falsely led to believe that they have consumer-controlled privacy.

Prepaid telephone cards provide an example of false privacy. Because the consumer buys the card from a kiosk or vending machine, the consumer assumes it has the anonymity of cash. But every time the card is used, a central record is made of the

card's unique serial number, the telephone number and the time.

Now, it's not too hard to discover who owns such a card by, for instance, searching the record for frequent use of particular numbers, such as a person's home or office.

It also helps to piece together the succession of similarly profiled cards used by the same person which can result in a surprisingly detailed history of a person's movements and associations over time. And yet consumers believe that privacy is user-controlled and are according in the use of the cards uninhibited.

There are other more blatant examples of false privacy. General purpose stored value cards tied to bank accounts, for example, are even easier for the operator to trace. But some have been advertised to consumers as providing the privacy of cash.

Similarly, credit card use on the Internet is fully traceable by those operating the system although some of them have claimed privacy as a feature.

Today's paper-based bank notes, technically referred to as bearer instruments, provide consumer-controlled privacy and payments. But their two-way anonymity, which protect both the payor and the payee, can facilitate most criminal activity.

All of these problems can be overcome by the new privacy interaction technology. An example is eCash, the first digital bearer instrument. An eCash coin is simply a number that's worth a certain amount of money.

You get such eCash coins the same way you get paper money except that instead of visiting an ATM machine in person, you visit your bank's digital branch over the Internet.

Just like the ATM, you identify yourself and request a certain amount of money to be withdrawn from your checking account. Instead of issuing you electronic coins from an inventory, which could be traced to you later, the bank makes electronic signatures for you in a way that lets you protect your own privacy.

How this actually works with numbers can be illustrated with paper and envelopes. Just zooming in here, the bank, the blank coins are actually random serial numbers created by the consumer's PC. The PC hides or blinds them by placing them in envelopes, actually a layer of encryption, using secret keys known only to you and your PC.

The bank then signs these blinded coins, actually forming a digital signature. When they're returned, the PC removes the envelopes using its secret keys and stores the signed but unblinded coins on its hard disk. A merchant, who later receives those coins, forwards them to the bank and waits to hear back before accepting the payment.

To ensure that the coins have not been spent before, the bank checks its list of previously spent coins. Since they carry the bank's signature, the bank knows that it must honor the

payments to the merchant.

The bank does not know from which account the coins were withdrawn or the payer, since all the coins were hidden in envelopes during withdrawal.

Let me now briefly show you an example of eCash. You will notice in the upper right the advanced bank wallet which is part of the eCash software. It shows that you have a hundred dollars Australian on your hard disk. Now a number of other banks that are involved with eCash including Deutche Bank, Europe's largest bank; the largest banks in four other European countries; some major Japanese banks, Imora and Situra; and others.

But let me just go through the steps. You choose something you want to buy from the shop. Then in the lower right you select the eCash payment option. Your software displays a dialogue, which asks for your agreement to all the transaction details included in it. When you click okay, you will notice in the upper right that the money has been deducted from your hard disk and you've made the purchase.

This approach gives the consumer protection. If your computer system breaks down, you can get all your money back from the data stored on the network by using the secret key. Only you can spend your money and noone can stop you from making payments, no matter what kind of mistakes your bank makes.

You have complete computerized records and digitally signed receipts of every payment made. eCash protects the interests of society as well. You can, for instance, always get the equivalent of a cancelled check from the bank simply by providing the serial number of the coin and asking the bank to issue a signed copy of its record of who deposited it and when.

This record could then be used to incriminate an extortionist, someone making or taking a bribe, or the acceptor of a payment in a black market scheme. What kidnapper after all would accept payment by check?

This one-way privacy makes the system unsuitable for so-called criminal use. Since this money must be deposited to determine if it has not been claimed by someone else, money cannot be held outside of bank accounts after it is paid, giving tax authorities up-to-the-minute information on revenue received by each participant.

The irony is that ill-informed concerns are raised often in the media about alleged, but untrue, dangers, such as aiding black markets or tax evasion that Internet electronic cash poses to society.

Although it is true that paper money is the life blood of criminal activity, and only by replacing it with something offering protections to society like those of eCash can we get a solution to criminal use.

And with consumer protections of eCash, we can do that in a way that would be acceptable to a society with our values. To use eCash over the Internet, all you need is a PC and the

downloadable software. But other platforms, including Smart Cards used by consumers at the physical point of sale, are also growing in importance.

If you put your Smart Card into a reader at a vending machine, you have no way of knowing what it is doing with your card. Its display might show that it's taking one dollar in payment for a soft drink, while in fact it's taking a hundred dollars or even checking your medical record or changing your car insurance.

What you'd really like is to have all the protections of eCash. In particular, you should be able to decide if you want to answer any request that is made. And if you do answer it, you should be ensured that only the transaction you have agreed to is done, only necessary information is revealed, and you are automatically supplied with complete and convincing records.

All this can be achieved with a hybrid, the main part of which would still be a PC although it might be in the form of a wallet, a pocket agenda, or personal digital system used for many other things. It would act as an intermediary between the tamper resistant card inserted into it and the outside world with which it communicates over an industry standard infrared.

The payment or other credit request would be communicated to your wallet and displayed by it to you. You would authorize it by pushing a button on it. This hybrid can give all the protections of eCash to the consumer and the same security, even off-line to merchants and organizations as cards alone.

Trials on actual eCash technology in wallets like this have been conducted at the European Commission Headquarters. You see the display, buttons, the infrared communication capability, and the Smart Card reader.

The highway speed road toll systems we developed with AMTAC in Dallas also use eCash technology in a hybrid except that the driver doesn't have to push the pay button because it completes the entire transaction in less than a yard of road travel even at a hundred miles an hour.

These protections are not only applicable to payments. For instance, they allow secure loyalty programs with members known only by their credentials, or they let customer surveys and even elections be conducted both securely and privately.

As explained in my Scientific American article of August 1992, we have been able to prove in theory that a similar solution can be realized for any information processing function used today, provided that there is a consistent policy of inclusion.

As information technology becomes a more important part of our lives, interaction privacy will become a central ingredient of democracy in cyberspace and critical to supporting our national values. In an increasingly competitive world marketplace that's racing for leadership in electronic commerce, interaction privacy can give the U.S. great advantage.

A small central effort, however, could make an enormous difference in realizing this opportunity. Simply establishing suitable definitions would help lead to more truthful labeling, healthy guidance, and more rapid convergence of this developing industry.

Thank you.

MR. LUDWIG: Thank you very much, Mr. Chaum. That was very illuminating.

Now let me ask the rest of our panelists to comment on this important issue beginning with Miss Culnan.

MS. CULNAN: And as a introductory note, my remarks are my own and do not necessarily represent the views of the Commission.

I want to talk briefly about three points. The first two are really tools that you and business can use to protect privacy and address the trust deficit. I will say a little bit about that and conclude with some recommendations about the government's role in all of this.

I do think that the main barrier for the widespread adoption of electronic money will be consumer trust or competence in these new payment systems, and that privacy through fair information practices and anonymity are the ways to build that trust, and without trust these payment systems aren't going to catch on.

So first I'd like to speak about some of the issues related to anonymous electronic money. I think it is important to have some forms of anonymous payment systems. I know they're law enforcement concerns but I think these can be addressed.

The majority of consumer transactions are small cash transactions in terms of volume, not dollar amount. Examples are: people who stop off to buy a newspaper or a cup of coffee on their way to the meeting this morning and that having the choice to make anonymous purchases will be important to consumers.

If people find that every cent they spend is being tracked, this is not going to be an acceptable alternative. The issuers can deal with the law enforcement concerns by designing electronic money to minimize the potential for crime and money laundering, and the risk to consumers, because if your money is anonymous, if you lose it it's the same as losing your cash.

By limiting the maximum value that can be carried on a card to $500, one can't launder much money. Limiting the amount of money that can be transferred from a particular bank account to one or another account in a particular day can also build in some safeguards against unlawful use.

For non-anonymous E-money when there is an audit trail that can be provided by either the issuer or by the merchant, fair information practices need to apply. I know that these are familiar to the Federal Trade Commission and hopefully to the Task Force as well.

You can summarize these in two lines. Say what you do and do what you say. Why are they important? They help overcome the

trust deficit. Because when companies say they observe fair information practices and in fact do this, they are saying to consumers you can trust us.

And they serve as a substitute for the kind of first-hand knowledge that we have in our personal relationships when we learn to trust people through experience. You can't do this with banks or with other large organizations. You need these surrogates to tell people that they can be trusted, and fair information practices serve that function in the privacy arena.

For business, it is a source of competitive advantage because people prefer to do business with firms they can trust and should be able to gain more customers. People also are more willing to disclose information when trust is part of the payment system.

A current survey was released here at the Federal Trade Commission during the June hearings that says in the electronic payment arena there really is a big consumer trust deficit. People aren't rushing to start using these systems. I think people aren't quite sure that they can trust them.

So what should the government do? The one-size-fits-all approach to electronic money is not going to work in a competitive marketplace that's characterized by diverse consumer preferences.

There need to be a lot of experiments. There may be some people who would like to have a cash card where they get a receipt or some kind of a statement every month telling them how they spent their money, just like there are some people that like to record every cent they spend into Intuit or another software program.

There are others who won't. So I think the Clinton administration was right in its framework for global electronic commerce by deciding that it is too early to regulate electronic money because things are changing so rapidly.

But government clearly needs to keep a watchful eye for fraud abuse and criminal activity. Government should partner with industry on consumer education about how these new forms of money work, then risks, and the tradeoffs. Then people would not assume a piece of plastic is an anonymous cash card, that works the same way as a credit card with the same kinds of limits and protections.

The government can clearly use the bullypulpit to push for responsible use of fair information practices and other rules to balance consumer concerns for privacy with the fair commercial uses of consumer information.

I urge the Task Force to look at the model established by the Federal Trade Commission for the Internet. It has been enormously successful in bringing people to the table in meetings throughout the year.

There's been demonstrable progress over the two years the FTC has been doing that. And I would think we could see the same

kinds of results in the electronic payment center.

MR. LUDWIG: Thank you very much, Miss Culnan.

Now let me turn to our next speaker, Miss Grant.

MS. GRANT: Thank you. I'm pleased to be participating in this forum on behalf of the National Consumers League, the oldest nonprofit consumer organization in the United States. The League has been concerned about fairness in the marketplace since its founding in 1899. In our view, consumers are the owners of their personal information, and that information has value.

If there is to be fair trade in consumers personal information, its value and the interest of consumers must be recognized. Consumers shouldn't be compelled to sacrifice their privacy to benefit from new technologies such as electronic cash.

We have an unprecedented opportunity to build consumer privacy and security into these new electronic cash payment systems, rather than being in the all too familiar position of closing the barn door after the horse has escaped.

Moreover, systems like eCash and Smart Cards can offer consumers more control over their privacy than is possible in other kinds of payment systems. Consumers are suspicious of technology, a fact borne out by the recent privacy and American business survey on computer users, because they feel that it's out of their control.

The key to the success of electronic payment systems will be consumer-controlled. Starting from the base line that consumers are entitled to privacy and security, these systems should be designed to give people the ultimate control over who they provide information to and how it's used.

Government should set basic principles to guide businesses as they build consumer privacy and security into their systems. Consumers must be asked to provide no more information than is needed for a stated purpose; be informed of exactly how their information will be used; be given real privacy choices that they can easily exercise; be given easy access to their information and the ability to correct inaccuracies; be guaranteed that their information will be adequately safeguarded; and be able to identify and hold accountable those who fail to honor their privacy rights.

In electronic commerce it's especially important for privacy practices to be transparent and for good systems to be created to respond to consumers' questions and complaints because by its very nature this type of commerce is invisible.

For consumers to trust these payment methods, they must understand them and believe that they have control over them. Putting on my fraud hat for a moment as director of the League's National Fraud Information Center, I am concerned about scenarios, such as consumers using eCash to pay someone posing as Readers' Digest for a subscription renewal, when that person is not connected with the publication at all.

This is a frequent type of telemarketing and Internet fraud

that we hear about. While I understand that merchants will not be able to opt to be anonymous, I wonder what procedures will be used to validate the merchants before they can participate in the electronic commerce scheme, revisiting the days that many of us went through when there were great concerns about consumers giving their credit cards numbers to con artists and we had to do a lot of consumer education in that regard.

And we have seen con artists in fact shift to other means of payment to get around that consumer education and around the merchants type of safeguards.

And since some transactions, for instance, magazine subscriptions will not allow the consumer to be anonymous, I do worry about how the information that they provide especially to con artists will be abused.

Finally, it's clear that there is going to need to be a significant effort to educate the public about these systems. And by the public I mean both consumers and businesses. We need to educate people about the need for security, and fair information practices.

The National Consumers League intends to be an integral part of that effort and we look forward to working with people in government and the private sector to make sure that electronic payment systems are an attractive option for consumer transactions.

MR. LUDWIG: Thank you very much.

Now, Miss Johnson, we'd be interested in the law enforcement perspective.

MS. JOHNSON: It's a pleasure to be here. Inviting a law enforcement person to a privacy related topic is what we refer to as a skunk at a garden party. We called ourselves that first but have been subsequently told that it might be true.

But I hope that my remarks will make my presence at least tolerable. FinCEN in the Department of Treasury is the youngest law enforcement agency, created in 1990. I thought it be useful to tell you a little bit about who we are.

We're a network. Even though we reside in Treasury, we are represented by people from 22 different federal agencies. Our mission is a smaller slice of a larger pie, which is to prevent money laundering and other types of financial crime.

We do that by collecting and disseminating data in support of law enforcement investigations. We do that by writing and administering 31 CFR 103, the U.S. Bank Secrecy Act. It is really a misnomer because it requires entities, businesses, and financial institutions, which provide financial services to keep certain records and file reports.

We have been looking at the privacy issue for about two years in terms of money laundering, fraud, counterfeit, and other crimes. We are humble enough to believe and know that most issues on the macro level will not be decided by FinCEN or any one particular Treasury law enforcement agency, such as IRS, Customs,

Secret Service, and Alcohol, Tobacco, and Firearms.

But the ultimate decisions may affect how we are able to do our job. Our philosophy has been don't act hastily and impede competition, but try to keep a seat at the table so that we don't want a problem to occur and come in after the fact.

We have worked closely with the industry and have received tremendous cooperation. They have been trying to help us work through what I think our concerns. This is what we term the paradox of secrecy, things that make these systems good; their security, their efficiency, and their speed are great from legitimate commerce.

They may be great for my customers who are the criminals. Granted, we understand that these systems are still in their infancy, low-dollar-value transactions, consumer oriented, not the types of things that the Bank Secrecy Act has in the past or ever would want to contemplate records on who buys a subscription to what.

That's why we have thresholds in existence and have been working to reduce our existing burden on financial institutions.

We do have questions and want to continue a dialogue whether these E-money systems develop in such a way, and, it may be premature, they are providing financial services. We ask the industry and others to help us with what, if any types of precautions should be put in place for financial crime and fraud, how will this affect our existing law enforcement techniques, do we need new ones, and do we need to adapt?

And on international jurisdiction how will we ensure a level playing field. Currently we talk to other countries about their antimoney-laundering programs, knowing that the United States or a few countries have a significant program, other countries may not, and some of the bad money or activity may move offshore.

That ultimately hurts us as well. So we're a little concerned with staying abreast of things to ensure a level playing field. We have done a few things. We have continued to work with the industry. We had a colloquium in New York where we talked about issues, a lot of issues unrelated to money laundering. We have worked with the Financial Action Task Force, which is a group of 26 countries, the major financial centers, in Paris.

They have adopted 40 recommendations against money laundering. This year we were able to include a new one that said countries should look at the implications of E-money, with your partners in the industry.

We also recently did a series of simulation exercises with the Rand Corporation. The resulting paper will be probably presented sometime in the summer. Industry, law enforcement, and consumer representatives gathered to discuss the possible effects of E-money.

We're interested in a level playing field for all. We do not want to impede any development of good systems. We understand

that things are still moving at a relatively steady pace, and that we need not be hasty and tell everyone to overlay a regulatory environment that is either incorrect or burdensome to the industry and doesn't really provide us what we want.

I bring that message to you in the hopes that I can convince you. We have taken a single step, however. Recently we leveled the playing field for those depository institutions or financial institutions other than banks, check cashiers, money transmitters, casinos, and others. We have a statutory mandate to bring them under the rubric of antimoney-laundering measures and recently issued a series of notices of proposed rulemaking for that.

One proposal is a requirement that all providers of financial services that are not banks register with the Department of the Treasury. We have proposed that potential E-money issuers should register with the Department of the Treasury.

We are not doing it in a vacuum. We have a series of partnership meetings scheduled, the first of which will be held on July 22 at FinCEN. You're all invited to attend if you would like to discuss this issue among others.

I am thankful that we were allowed to participate. I hope that maybe I don't smell as bad as every skunk and that you will continue to keep us informed and let us have a seat at the table.

MR. LUDWIG: Thank you very much, Miss Johnson.

Miss Koehler.

MS. KOEHLER: I am Janet Koehler, Senior Manager for Modernized Product Development at AT&T Universal Card Services.

However, I'm here to represent the Smart Card Forum and neither AT&T nor Mondex. In the audience today also representing the Smart Card Forum are Diane Daryl, Executive Director, and John Burke, General Counsel.

The mission of Smart Card Forum is to accelerate the widespread acceptance of multiple application of Smart Card technology by bringing together in open forum leading users and technologies from both the public and private sectors.

The forum has 61 principal members and 107 auditing members from business, including banks, telecommunications providers, software companies, equipment providers, and car manufacturers, etc.

Twenty-seven state and federal agencies are members as well. Among the forum's objectives are to lead the Smart Card industry forward by establishing a vision for interoperability and to develop cross-industry positions on issues relevant to technology, business, and legal and public policy.

On behalf of the forum I thank you for the opportunity to talk with you about our shared objective, understanding consumer issues that arise from electronic payment technologies and what the industry can do to address these issues.

When I spoke to this committee in April, I reported the

Smart Card Forum was finalizing a privacy policy to guide its members in responding to consumers' needs for confidence that their stored value transactions, using Smart Cards, would be protected from unwanted privacy intrusions.

The guidelines were developed through a process of reviewing recommendations of governmental bodies, looking at examples from other industries, requesting input from member organizations, and having early discussions and a final review of consumer advocates.

In May, the Forum approved and announced these guidelines. The guidelines addressed respecting the privacy of expectations of consumers, ensuring that the data is as accurate, up-to-date, and complete as possible, promptly honoring consumers' requests for information that a company has about them, and enabling them to correct inaccurate personally identifiable information, limiting the use, collection and retention of customer information and applying appropriate security measures to protect customer data.

Consumers should be given a means to remove their names from a company's telemarketing, on-line, mailing, and solicitation lists. If personally identifiable consumer information is to be provided to unaffiliated third parties for marketing or similar purposes, the guidelines say that a consumer should be informed and provided the opportunity to opt out.

And the third-party should be required to adhere to equivalent privacy standards with respect to that information. Smart Card service providers should implement policies and procedures to limit employee access to personally identifiable consumer information on a need-to-know basis and to educate employees about privacy standards and employee's responsibility to protect consumer privacy and to monitor employee compliance.

Copies of the guidelines are available outside on the table. When Smart Cards are used on the Internet, the emerging privacy protocols or standards will complement the Smart Card Forum privacy guidelines.

We have sent copies of the guidelines to all of our members and will have a session at our annual meeting in September to help our members identify and overcome privacy and related barriers to consumer acceptance.

During the same week that I met with this committee in April, I also participated in the Federal Reserve Board's Consumer Advisory Counsel meeting. The Counsel was discussing the application of the Electronic Fund Transfer Act to stored value products and the need for disclosures to consumers.

Counsel members, who included industry and consumer representatives, agreed that it is in the best interest of consumers and stored value card providers to tell consumers what they are going to be receiving, what limitations there are, what their charges are, how to get a card replaced if it is lost, what to do if the transaction or the rights doesn't work as intended.

But at the same time the industry members, who are familiar with stored value cards, express the belief that it is premature to prescribe a particular form of consumer disclosure particularly when stored value products are not very far down the read to development and implementation.

One example is the question of what a consumer should do if a stored value payment transaction is not completed because of, for example, a power blackout.

Since many of the stored value card applications are still in development, there are a wide range of possible approaches to this problem. Implementing a specific regulation, which is based on a trial version of one payment application, could seriously impede the growth of innovative solutions to this problem and could conceivably stop the development of a particular technology altogether.

When the Smart Card Forum's Legal and Public Policy Committee met last month, we agreed to take on the challenge of developing disclosure guidelines for stored value card providers to use in deciding what they need to tell consumers about their products, so that consumers will understand their rights, responsibilities, and the products that they will be using.

In fact, we have established a subcommittee on disclosure guidelines and will be gathering information from a wide range of industry and consumer representatives. We welcome the guidance and input from this Task Force.

It is indeed a challenge for all of us to develop guidelines that can be helpful across some different products with very different features which are still evolving.

We want to be sure that the guidelines work well across all likely forms of products and do not advantage one system over another. We won't know how long it will take until we're further along in the process; we're just beginning.

Undoubtedly our initial product will be a little less than perfect and perhaps not as robust as it needs to be. I think it will be a process of trial and error and continuous improvement.

We are reviewing the discussions and proposals of the regulatory and legislative bodies that have addressed these issues, including the members of this Task Force last month, and that will be helpful to us.

Thank you for the opportunity to discuss the work of the Smart Card Forum, and we look forward to continuing the dialogue.

MR. LUDWIG: Thank you, Miss Koehler. Your group's focus on these issues is commendable. I did wonder when you talked about the policies you're working on, are you proposing any mechanism to ensure that if somebody signs up that they volunteer to participate in that set of policies that they're followed?

MS. KOEHLER: As with any broad industry association, these policies can be principally voluntary. They provide a guide. And we hope that through perhaps moral suasion, just the fact that so many companies were members of the organization that they have to

review and sign off on the guidelines before they're published, that they will be making a commitment toward that. And we will certainly see that as we roll out.

MR. LUDWIG: Thank you very much.

Miss Mulligan?

MS. MULLIGAN: It's a pleasure to be here. I feel like I have spent a lot of time in this room this summer. No offense, I'm looking forward to August.

We just spent four days discussing privacy on-line before the Federal Trade Commission. And while E-money was not explicitly part of that discussion, it was implicit in the reason we were having the discussion that the range of, the area of commercial transactions, for lack of a better term, is where the rubber hits the road; or I think probably even more appropriately, it's where those digital tracks that you're leaving all over the Internet head right to your door.

So I think that it's useful to think about the principles that were called from the FTC proceedings not this past June, but the June before, and were actually explored more fully and more thoughts about how they could be implemented in this most recent set of hearings.

The principles that came out of last June's hearing as core components of developing a privacy paradigm or useful way to think about privacy in the on-line environment where notice or disclosure to consumers about the implications, the information being collected, what purposes it would be used for, to whom it might be disclosed and the general privacy implications of the information, choice or control, the ability to make decisions based on that information in a meaningful way, access to data that others have about you, and security. And I will steer clear of that, because I know our next panel is going to address that issue more fully.

I think that it's fair to say that the financial marketplace is a fairly aware of privacy, that we have had years of surveys that have shown that this is an area where consumers are more aware and more savvy about privacy.

That kind of diversity of payment mechanisms that we see in the traditional marketplace reflect some of those concerns. And I think that consumers do choose between payment mechanisms understanding the consequences and traceability.

That said, data collection is growing and moving in a very important way. But for most consumers, the transactional data that was collected about you yesterday at your credit card company or at your bank or at some other financial-type institution is now possibly collected, not only there, but also at the scanner at the grocery store, at the Web site, and at the retail level.

So that the diversity of information both collected, its quality and its quantity, and the fact that there are multiple places where that data may be captured and stored is really

changing some of the privacy concerns.

The terms E-money and electronic payment systems I think is rightfully pointed out. They are widely different systems that are available. And we are seeing products that are familiar to us in the off-line world: credit cards, debit cards, and stored value cards, like a traveler's check.

We're seeing those both offered in the on-line world. Probably most importantly, we are seeing those merged. The consequences were really evaporating. The traditional ideas about the types of protection about records being created, and other activities are disappearing because the digital environment. The on-line world creates records of your activities regardless of which form of payment mechanism you choose to use.

So if we are to have the options that we have had in the off-line world in the on-line world, those have to be crafted by policy, because they do not necessarily flow by your choice of the tool.

I just want to note as I think Dave did and I think others will that eCash or other types of things that are like money--and when I say like money, they are fungible, universally accepted, securely backed, and equally valuable for transactions between me and a grocery store and between you and I. Those play an incredibly important role in our economy.

Part of that role is in protecting anonymity and privacy. I think one must be vigilant to have that in the on-line world. As Allen Greenspan noted, there is no doubt that there is a market for privacy, if privacy is available.

I would encourage you to see that as a real mission in this area. In reviewing the electronic payment systems and their literature on how data is collected, most of them are forthcoming about the flow of information about me to others with who I am engaging in a transaction.

So what the merchant gets access to may be clearly stated. What is much more opaque is what the system is doing with the money, and the transactional data.

A quote in the Security of Electronic Money Report states that the full transaction information is transmitted to a central point. The issuer will probably be able to relate transactions to particular consumers fairly easily. This could reduce the level of consumer privacy.

It is a huge understatement to say “reduce.” I think that will drastically change the way in which consumers engage in the marketplace and the consequences of that.

Today individuals are rarely given information that explains the privacy implications of a given payment mechanism in a comprehensive or a compelling way.

I do not intend to dismiss the efforts of the Smart Card Forum and the credit and financial institutions, because unlike many of the Web sites that Marc Rotenberg and I have reviewed,

they have made an effort to educate people.

The reality is, though, if you ask most consumers what the difference is between choosing a debit card, a credit card, and a cash payment, they may note the delayed payment from using a credit card.

But few of them will tell you about the privacy implications of making that choice. As we move into the on-line world that the quality and quantity of information can be collected by merchants and others about not just what you purchase, but what you pick up, what you consider, what you read, where you are shopping, where you are spending your time, and to whom you are placing phone calls. Without an effective consumer education component to really explain to people what the consequences are of these different choices, privacy is going to severely drop off and consumers will suffer.

So I look forward to hearing more. And I encourage you to ask questions of people who are developing the systems, not about what information is available to people with whom I'm transacting with, but about how the information collected by the system is being handled; how is it being stored; where are the access points; where are the vulnerabilities; and where is it being backed up, because I think those are the real questions.

MR. LUDWIG: Thank you. Mr. Rotenberg.

MR. ROTENBERG: David introduced a new term this morning, and I am going to coin a new phrase, I think what's needed for consumer acceptance of new payment systems is the development of robust anonymity. I'm going to be making three points this morning to support the concept of robust anonymity.

The first point is that anonymity is the default for the vast majority of consumer transactions. Mary Culnan made this point earlier today. Eighty percent of transactions in the United States, according to a 1995 Treasury Department report were cash based.

Therefore, it's important to recognize that the confidence and the assurance that people associate with the use of cash could easily be lost if new payment systems require forms of identification.

The second point is that the technology to promote anonymity and the implementation of anonymous payment schemes reduces regulatory burden. Let me explain this point.

Mary Culnan mentioned fair information practices, which are the principles that are broadly associated with the obligations to protect personal information that is collected. Those fair information practices can take the form of industry guidelines or professional obligation, often that take the form of law, statutory restriction and the use of how personal information may be used.

This is true in the banking era. This is true for credit reporting. It's true for video rental records, for cable subscriber records. When organizations collect personally

identifiable information, they often must comply with certain legal obligations about how that information may be used and subsequently disclosed.

Therefore, one reason that anonymity is so attractive is not only on the consumer side, but also on the business side and the organization side because it diminishes the obligations that would necessarily result when an organization chooses to collect personal information.

My third point is that anonymity is very much desired in the on-line world today, in the Internet world, in the world where so much of the focus is now on new forms of payment, new forms of commerce, and new forms of economic opportunity.

There are several reasons for this. One may be simply cultural. The Internet grew to promote wide-spread anonymous activity and interaction. In our survey this year for the Federal Trade Commission, we looked at a hundred of the top Web sites. We noted that, although few had adequate privacy policies, virtually all allowed users to use the resources, visit the Web site, and download the information without disclosing their actual identity.

We suggested, based on the survey, that this de facto practice of protecting anonymity on the Internet was one of the things that was protecting privacy today. That could well change.

A second point in support of user desirability is simply opinion polls. The most comprehensive polls have asked the question straight out of users of the Internet whether they support anonymous payment systems or user-identified payment systems?

The semiannual poll by the Georgia Institute of Technology, which is available at our Web site, found that, on a scale of one to five, users expressed a preference of 3.9 in support of anonymous payment systems and 4.4 spoke about the right to act anonymously. It was one of the highest levels of agreement among the 15,000 people who were surveyed on their attitudes about use of the Internet.

So, there is clearly a strong recognition of the need for anonymity.

Now, another significant area in new payment systems is concern about fraud and traditional consumer protection. There is an interesting area of overlap between anonymity and concerns about fraud.

Although the lack of accountability in some anonymous payment systems will allow certain types of crimes to occur, one crime which clearly does not occur in that environment is identity theft.

This particular problem of identity theft, which leaves individuals virtually without any limitation on the exposure to personal risk is a significant problem in this country today.

Anonymity could be important in trying to limit that

particular type of criminal conduct.

Robust anonymity requires reliability and trust. People have to look at anonymous payment systems with the belief, well grounded, that the systems will work as they're represented.

The second requirement is that their adoption for consumer purposes has to be widespread and widely accepted. It won't work if anonymous payment systems are pushed to the margins or considered to be special cases of other types of payment.

And the third, I think anonymous payment systems need to address law enforcement concerns, because of the money laundering risk. David Chaum effectively explained how the one way anonymity of his system addresses the law enforcement concerns it protects the identity of the consumer, but allows for accountability for the merchant and defeats blackmail and extortion systems. Now, if these three criteria can be satisfied, I think we will have robust anonymity; The key to consumer acceptance of new payment systems.

MR. LUDWIG: Thank you.

Now our last panelist of the first panel, Miss Sullivan.

MS. SULLIVAN: I'm the Director of Government Relations for the Consumer Bankers Association. We represent the nation's largest financial institutions on consumer and retail delivery system issues.

In this capacity we have a committee that works solely on technology and the delivery of retail products and services. This committee identified the issue about privacy about three or four years ago and created industry guidelines.

We adopted our guidelines in September 1996, after three years. It wasn't easy, because balancing business interests with consumer interests is very hard.

It's also because of the technology changes. What is good today may not be helpful tomorrow. In December 1996 we had a workshop for bankers telling them how to implement the guidelines.

We plan another workshop this fall. The American Bankers Association just adopted one that is very similar to ours, the Smart Card Forum. I think the basic principles are something we all agree on.

Mr. Ludwig, you have identified a problem enforcing the guidelines. We don't want you to pass regulations. I think there are 82 bills now that talk about consumer privacy in the legislature.

A month and a half ago there were 52 so everyone is very interested in this issue and with good reason. Mr. Greenspan recently said that there ought to be industry self-regulation. One of his reasons, and our main reason, for it is that self-regulation can change because of market forces.

When legislation is passed, it's much, much harder to change. This is an area that we think really needs to be very flexible.

We are working with the ABA and other trade associations to see how we can best get banks to adopt these privacy guidelines.

Many of them have our policies. Many of them have policies in their code of ethics. The policies may apply to smart value cards, smart cards, or perhaps credit cards. Our goal is to get them to be adopted throughout the retail industry. And that's not quite as easy, because of computer problems or the expense actually involved in getting all the computers to be able to do everything that we'd like them to do.

That's part of promising something and being able to deliver that at the same time. But we are working on it. We do think that the regulators have a very important place in what's going on right now, and that is for consumer education.

Part of it is the forums that have been held. Certainly what the FTC has been doing is important because this is not really just a bank issue. This is an issue that affects anyone that has a computer and the technology to gather information, use it, and analyze it as a consumer.

It's really good that more than just banking people are working on it. We'd like you to consider perhaps a role for educating consumers on what is going on, not only what a Smart Card looks like or what it could do, or what banking on the Internet could do, but what are some of their options for privacy.

Because everyone in this room understands what can be done and is being done. And I do think that it is here; it's not coming, it's here and it's been here for years, all of the databases and all of the information that's available about us.

Just as the regulators worked with people and educated them about the uninsured aspect of investment products, they could work with groups of consumers. The industry would be delighted to work with them and educate consumers about privacy.

Consumers ultimately will push the industry to adopt guidelines that will benefit both. And that's because consumers have to be able to trust their institutions, and I believe they will.

It's important to the banks to have that trust because it's important to them to continue to do their business.

No matter what we do here, we have to consider what is going on in Europe. Although there are competitive aspects to what's going on in the European union, the member countries have adopted some strict consumer privacy guidelines.

The administration is working with the European union on different aspects of the use of customer information. And I think that the recent paper by the administration acknowledges that. We have to be concerned about that as well as we go ahead.

MR. LUDWIG: Let me begin with one question and give everybody a chance to ask their questions.

Are we talking about all information? Is there a way to marry concerns of the law enforcement community with concerns of

consumer advocates in terms of every bit of information? Are we really talking talking about robust anonymity? Are we talking about all information?

MS. MULLIGAN: I'm not completely clear on your question about whether it's all information. Most of our problems we have tried to focus on applies to transactional data created through payment mechanisms.

David Chaum's example offers payor anonymity, but does not offer payee anonymity. It probably comes closer to addressing some of the law enforcement concern.

At least when you're dealing with institutions and providing some of the protections for anonymity for the consumer, it doesn't provide the kind of fungible one-to-one capacity that you might be looking for between consumers when both payor and payee are anonymous.

That would reflect the traditional marketplace. So there may be, as the law has carved out specific areas, whether it's the $10,000 transfer or other types of reporting requirements that we should be mindful of reflecting what exists today as we move forward.

Marc rightfully pointed out, as did Mary that what exists today is really a defaultive anonymity and that when consumers make choices for other purposes, such as because I want to defer payment or I want somebody else to maintain my money so I don't have to walk around with it that we make some types of knowledgeable decisions that balance the costs and benefit to ourselves.

So I don't think it's necessarily all or nothing. The choices have to be very specifically made and thought out.

MR. LUDWIG: Mr. Chaum mentioned that payee information should not necessarily be included from his perspective. And Miss Johnson said that for a large amount of transactions, information is not abundant.

MS. GRANT: There are legitimate societal concerns and that part of the price of being in business is making at least some information available about your businesses, the payments that you receive, and what happens with that money.

So I don't have any problem with precluding businesses from being able to get complete anonymity because I think that is necessary to protect law enforcement concerns.

I think that on the consumer side of it, it's up to consumers to decide what information they are concerned about. Sometimes we hear the doctrine of do-no-harm promoted.

But that leaves it up to the holders of consumers information, who have received it through various means, to determine what's harmful and what isn't, rather than for the consumers themselves to determine.

So in that case, the ultimate decision about what and how information about the consumer should be retained should be up to the consumer.

CHAIRMAN PITOFSKY: This is the heart of the matter about robust anonymity. Let me give you two situations that perplexed all of us.

One is that drugstores collect information during payment as to who is using what prescription. Most people feel that for personally identifiable information to be sold by drugstores to the drug companies without notice of consent is a real invasion of privacy. Maybe some people don't agree with that, but I'd like to hear about it.

In the other situation, the drugstores as a group aggregate the information thereby eliminating personally identifiable information, but sell it as a commercial transaction to the drug companies.

If the consumer owns the information, you would be concerned about doing that without the permission of the consumer. On the other hand, one wonders really about the privacy invasion in that situation. When we talk about robust anonymity, would we include a situation like that where personally identifiable information is not involved?

MR. LUDWIG: Could you make your question more complicated? What if the aggregate information sold to drug companies was actually helpful disease control? How much of a vaccine is being sold in the aggregate in the metropolitan D.C. area, for example, as compared with some other area?

MR. ROTENBERG: I actually don't think it's a hard problem and I think you have suggested the answer. Simply that when the information is not personally identifiable, the privacy interest really goes away. It is for all purposes as if it were anonymous. Aggregate data is essentially anonymous with respect to the identity of individuals.

So at least from my perspective I would not see any problem in the situation. The problem which you have suggested, which is a little more complicated and forces us to engage in some balancing, is that there are circumstances where personally identifiable information is disclosed perhaps without notice and consent in the medical field is one for the purpose of providing a benefit to the individual.

And then we have to do some hard work. But this discussion really focuses on these payment systems. And these payment systems represent a more narrow category of issues we need to consider.

An example is the new highway systems that David Chaum has been involved with, and whether the toll records when you travel on a highway are user identified or anonymous. We are talking about communication systems. When you buy a telephone service is that payment user identified? I think those were the problems we were asked to look at.

MS. MULLIGAN: Marc and I are in general agreement about where the individual's privacy consideration may end. But because you specifically laid this out in the medical context I

feel a need to add, that there are some other considerations with data.

Some people have talked about group privacy interests. And the medical context is one where this really plays out. Although the data that's collected may be stripped of information that identifies you as an individual, it may still identify you as a member of a specific type of group of people. That information then is used to discriminate, for example, among types of people. In some other interesting ways, the availability of the information can be both used for very beneficial and also have some negative consequences. We've certainly seen this, for example, in the credit area and in the medical area with redlining.

While it may not be a privacy interest, there are some other interests to keep in mind.

MR. LUDWIG: That's an excellent point. We might even take it into the individual. I'm glad you mentioned the credit area because it really does crystallize this a little bit, too, as well as medical.

Early on, for example, it was viewed that collecting information about an individual's race in a credit transaction was viewed as a negative, that it could be abused in terms of the discriminatory decision making. Many in the advocacy community view it differently now; that is, the view is that the ability to collect that data is essential in terms of determining whether there is discrimination going on. Without the data, you can't do it at all.

I think this is a good example. It makes the group data issue very, very difficult.

MS. MULLIGAN: I think the Community Reinvestment is a perfect example of where the data is not necessarily good or bad. It is the use to which it is put. So it becomes a very challenging issue.

MR. LUDWIG: Does that then go to the issue of collection and use?

Perhaps the Chairman is wise enough to create the exact right example. But it seems to me that one can suppose cases where individual payment information about a drug, not group information, could be enormously valuable both for the individual in a health context and for the group as a whole.

For example, were they buying the effective drug or were they buying enough of the drug or were they buying the drug consistently. It could have broader implications as to whether or not there was effective immunization going on.

MR. CHAUM: It's not public, but I will make a little disclosure here without revealing the identities. Our company has developed a medical data privacy technology and it's actually in trial now in Europe. And it's specifically about prescription drug as you mentioned.

And what it does is it just is the example here; it allows

the anonymization of aggregated data. The purpose is to prevent what's called adversely interacting drugs.

So if you go to two different positions you might get some drugs that wouldn't work well together and could even be very dangerous. This system will find that out even though the medical records of the physicians are separated. It also lets the drug companies make sure that they don't waste money by giving people too much.

MR. LUDWIG: That would be on a individual basis? That would have to if you're going to talk about the, that would be not aggregate.

MR. CHAUM: Well, what happens is that the individual gets a kind of pseudonym which is not traceable to their identity but which is used at a central facility on-line to make sure that they're not the recipient of a conflicting drug.

MR. LUDWIG: What if they are? With the pseudonym, nobody knows who they are but the system turns up bright red and says --

MR. CHAUM: It tells the prescribing doctor not to prescribe that.

MR. LUDWIG: But the individual is still out there taking the drug.

MR. CHAUM: At the time of the prescription, it's the way that the system is set up. The physician checks on-line to make sure that this prescription is a good one for that person, that there is no allergy put on record and that sort of thing.

But I think it's important to distinguish between two kinds of mechanisms for privacy. And that's what I was trying to bring out in my preparation. You have got the type where the consumer is in control of the data, or you've got the situation where that data is in the hands of a third-party and we're trusting them to do the right thing with it.

You should distinguish also between when a merchant has access to identifying data about you, maybe not related to the payments exactly but for other reason, and when the payment system operator can recover this information about you. Those are different situations and they're sometimes mixed.

We heard here that if you subscribe to a magazine using eCash then you've given up your anonymity anyway. Well, not really. You give it up to that magazine publisher but not to the payment system provider.

So what we have done in the medical case is made it so that you don't give up your anonymity to the physician and really not to a central facility in fact. So that's different from just saying, if the user gets together they can put it all in one computer and decide what's a good use and what's not a good use because then you run into the verification of those uses.

The problem with privacy is that it doesn't run itself. It is just auditing as a control mechanism because the data can be leaked out. It can be used for say clandestine and covert purposes without being linkable back to its source and so forth.

And if privacy once compromised can never be recovered. It's a very sensitive thing. And the best mechanisms are those that keep the data in the hands of, say, the individual or maybe their trading partner as opposed to allowing it to be centralized.

MS. CULNAN: I think it's not going to work to have a totally anonymous world. There are situations where that's very important, but there also needs to be accountability in a lot of circumstances.

Striking that balance is often very difficult. That's one of the issues we are going to be grappling with in the Commission in terms of terrorism on the Internet. If you're always anonymous, how do you catch people?

So I also think that the law-abiding public doesn't always want anonymity but they do want choice. There are situations where people choose to use a credit card and have a payment that goes on their record because you get certain benefits from that.

That's because of the way that the marketplace works and also because of certain regulations that are in place. So on the consumer side, choice is really the key. But to make good choices, people have to have good information about what's going to happen to their information after it's been collected. The push is now on self-regulation and better disclosure.

But what's missing from this piece of the puzzle is that we do not enforce this. We do not have good enforcement mechanisms. If someone detects that someone is saying one thing and doing something else, the FTC will be happy to hear from them.

But aside from finding this out, there's no way to know. There is no auditing requirement in place if the market demanded auditing standards that could become a way of doing business for companies that wanted to attract customers.

On the business side, companies need to know how their customers are using their products, because you can't be in the dark. You need to know what businesses are keeping records. You need to know who's using your card and for what purposes, and what kind of businesses are doing what kinds of business with your customers.

But the issue here that gets a little bit away from the privacy is the issue of compatible use in terms of how the information is used. Is it used for ways that are related to the purpose for which it was collected? That is is a very important principle.

And then where are the boundaries on the financial services institutions, for instance transaction facilitators? They know not only about the customer, but also know about the companies. They can use that information in some people's opinion for competitive disadvantage because whose customer are you?

And that gets us off of the privacy track but that's another important business issue that the direct marketing association has had difficulty sorting that out to everyone's satisfaction.

MR. LUDWIG: Thank you very much.

MS. MULLIGAN: I had a very particular question about the public policy concerning this trial that you're talking about, Mr. Chaum. When the information is delivered to the consumer at the point where they get the second prescription, is it delivered on a piece of paper or computer screen or does the pharmacist in the white coat say I'd like to talk to you about something?

MR. CHAUM: Well, I'm sorry to clutter the conversation with the details of this particular application. I just thought it was so surprisingly relevant that I should mention it.

In fact, the way the system works is that there are computers at each physician's office. The prescription is entered immediately into the computer. It checks on-line to see if there is a conflict. So it's the physician who is able to notify the consumer or change the prescription.

There are a number of issues, not only adverse interaction, but also redundancies and abusive substances, all kinds of issues. So that can all be dealt with by the physician.

But the separation between your relationships with different physicians and the health care providing organization and so forth is maintained very strictly.

MR. LUDWIG: Miss Johnson.

MS. JOHNSON: Thank you. Obviously as a citizen I'm concerned about the privacy and confidentiality of medical records. And obviously wearing my professional law enforcement hat those types of drug sales are probably not the ones that I'm most interested in.

Our concern with anonymity of course would be the inability to identify people. Our present system has about 12 million reports of just currency transactions over ten thousand dollars. We think that's way too many. That's not even capturing the noncash activity.

So our concerns are more about being able to not identify a person. If systems were to permit this, which right now I don't think they do, a person could buy drugs in large amounts from someone other than a drugstore and not able to be identified or perhaps a drugstore that receives an excessive amount of payment that isn't necessarily consistent with the general business activity that they've done before or other drugstores.

I'm very optimistic that we're going to marry our law enforcement concerns with the industry because I think many of the developers are taking like David and Russ from CyberCash are taking the appropriate steps to protect themselves and be good corporate citizens.

MS. SULLIVAN: I wanted to bring up enforcement one more time. Once a bank has adopted a policy, whether or not the examiners can't look at the policy and see whether or not there is, are mechanisms in place for banks to comply with their privacy policy is?

And that may be one sort of regulation method of seeing

whether or not banks are, well, at least financial institutions. You might be able to do the same thing if there is another mechanism for the FTC to look at organizations that are also collecting information and developing privacy policies for their consumer customers. Certainly banks are so highly regulated already that that might be a possible alternative for enforcement.

CHAIRMAN PITOFSKY: One more effort to add to the complexity of the problem which doesn't need any more complexity. We're talking now about situations where personally identifiable information might be disclosed for good reason; either it helps the person who is identified or it helps law enforcement or it serves some other useful social purpose.

But then the question becomes who decides whether the invasion of the privacy is so small, and the social and the good purpose is so great, that we will allow the disclosure.

Now, that implicates the question of notice and consent. If it's such a good idea for the consumer, why don't we ask the consumer to give consent to the disclosure of the information, or are there situations where the social purpose like law enforcement is so pressing that it trumps any privacy concern?

That I think is where our set of issues will turn out to be. And I'd appreciate hearing reactions to whether you think consent is essential whenever personally identifiable information is transferred if it's used within the company to improve the company's product, I haven't heard anybody complaining about that.

It's the transfer. And of course, as somebody said, the rubber hits the road where the payment occurs because those are the people who accumulate the most information about the most transactions.

Should we take the position that without consent those transfers of personally identifiable information should not occur?

MR. CHAUM: Let me just add one important comment to set a stage for that to answer to your question because it is an interesting question. I have to agree with you, it's difficult.

When you build these systems, if you don't build privacy in, consumer-controlled privacy as to default, then you lost that opportunity completely in the future for everything. So given that you do build it in to the basic payments infrastructure then the consumer has the choice always to whether they want to identify themselves or not for particular transactions and to use various kinds of systems.

If you don't build it in to the basic infrastructure then you've robbed everybody of that choice and of course you have no hope of reaching the robust level of privacy. So I think that's important to mention. There seem to be some misunderstanding about that point.

Just because you have a mechanism that protects people's

privacy and lets them control it doesn't mean that they can't very easily give it up and in a very secure way prove who they are to various people for various purposes.

What's not so obvious is that you can prove that you're the owner of a particular say pseudonym. So without completely identifying yourself you can show certain credentials about yourself, that you are a repeat customer; have received certain degrees; or paid certain insurances.

Those limited types of anonymity are also interesting and possible based on an infrastructure that supports user controlled anonymity.

MS. GRANT: I'd like to respond to that as well. In the previous FTC privacy hearings I gave an example of a company that was offering music that you could order over an 800 number. You could set up an account so you wouldn't have to give your credit card number every time you called to place an order. The marking people in the company decided, after focus groups with consumers told them it is when the easiest number when ordering, the company would use social security numbers.

When the company announced this to consumer advocates, we were horrified that they would have these social security numbers for a purpose that was not required and that even the consumers didn't recognize the danger.

It wasn't even that, the company planned to transmit that information to others, although it would have been possible road for them to decide to sell that information but that employees would have access to that sensitive information.

It goes back to having a dialogue with consumers about why you need the information that you're asking for and having them make an informed decision about whether the benefits are worth the exchange of that information. If not, who they want to give their business to.

It also points out the need for a vast amount of consumer education. Because this is a situation where neither the business nor the consumers were making an informed decision about how to set this account system up.

MS. SULLIVAN: I wondered if I could ask two questions. We talked about consent. From the bank's perspective, I'd like to know what you mean by consent because we have opting-in and opting-out. That is of terrific importance to a financial institution and an issue that's been bandied around for years.

As someone who formerly was in market research, the concern that we had is that if you demand consent, an affirmative consent from a customer, we will only do this if you allow us to do that, which is the real definition of consent, then you'd probably get a response rate of 3 percent because people then have to do something about it, and often they don't do it. And not because they care about it, but because they have other things that they're concerned about. So the industry standard has been opting out. And that has been and mostly from a market

perspective because then you have more people who, if they care about it, will let you know.

If they don't care about it, then you're free to go about your business. I didn't know if when you used the word consent when you were talking, if you cared one way or the other. That was one of my questions because we care a lot about that.

Then, the second piece was often financial institutions work with third-parties to provide products and services. And those third-parties almost always are under a contractual agreement with the bank that they can't use that information for other purposes.

It's never simple to say if the bank uses that information or a bank holding company uses the information for its own development of products and its own service of its customers. Airline mileage is one example where information is being shared, but it's being shared for a very particular purpose.

And if anybody is thinking about how to do that, we'd like those pieces also to be considered.

Thanks.

MR. LUDWIG: Miss Johnson, do you want to address that? I know Governor Kelley has a number of other questions. But before we get to that, you have raised the opt-in opt-out issue.

Doesn't technology give us a way of jumping over the problem you pose is that you can't use an opt-in system because most people won't check the block and it will frustrate businesses' other needs.

Technology could conceivably solve that problem, because if you sign up for something, the computer can be rigged so that you simply can't finish the transaction without checking the block one way or the other. So it wouldn't be a case where it would be a completely uninformed decision, because they would have to address the issue depending on how you set up the program.

MS. SULLIVAN: That's a perfect example of why technology is changing so much that we ought not have any rules in stone. That can't be done today, but when transactions over the Internet become much more common, some sort of screen that a customer can use right away will become much more viable and people will use it. Right now I don't think that's particularly workable.

MR. CHAUM: Can I just interject one related point? If there is a framework of privacy, consumers will be more willing to respond to all kinds of inquiries from organizations that may only have these relationships.

With these organizations they can have intimate relationships, but anonymously. That's one of the things that privacy technology can really do. It can help improve the quality of marketing input in on-line situations eventually.

MS. CULNAN: I'd like to just back that up with one quick example. The Internet surveys that Marc Rotenberg referred to and also the privacy in American business found that most people on the Internet won't give or decline to give personal

information to a Web site, because the Web site didn't tell them why they wanted the information and what they were going to do with it.

Again, it gets back to trust. If you've done business with a company for a long time, you trust them and you're probably going to cut them a little more slack. You don't expect them to come back every time and ask you; it's very expensive for the business and it would probably be annoying to the consumer.

Through experience, if things are okay, you get to that first threshold because they tell you these are the rules. If the rules are okay with you, you opt in basically to the relationship and then things proceed from there.

MR. CHAUM: My point was more about the survey aspect. People often give biased answers when they're identified in a survey. If people are able to answer anonymously, you can get higher quality information. But I support what Mary said.

MS. JOHNSON: If there was a particular issue for the law enforcement example, we might want to consider advice and consent means not only if they do not consent that the information wouldn't go but then perhaps the transaction wouldn't be able to be completed. That was my only point.

MR. ROTENBERG: I was just going to briefly answer the question at the outset. Choice is a necessary but not sufficient condition for privacy protection. There are many other interests including the right to access the information and to correct and some form of remedy when the policy is not upheld that have always been reflected in privacy laws and policy.

It is a mistake to put so much emphasis on choice. It is a very narrow slice of the privacy pie. The other point that I want to make is that I really do hope we don't lose this thread of anonymity. There are a lot of steps being taken now to try to promote anonymous payment schemes.

David described some on the technology side. On the policy side I will mention that last week the White House Electronic Commerce Policy released the discussion of privacy protection which explicitly mentioned anonymity as a possible solution.

And I think more interestingly, the new multimedia law which was recently adopted in Germany sets out a requirement that companies which are providing businesses and services in the new on-line environment do so to the extent practicable to provide for anonymity so that consumers who want anonymity can get it.

It's a very interesting answer to what is the appropriate role of government in this situation. What the German government is trying to do is to jump-start some of these anonymous payment systems by saying that if you're going to offer the services you have to provide privacy that as a consumer option.

MR. LUDWIG: Thank you.

Governor Kelley?

GOVERNOR KELLEY: Mr. Chairman, when we started this morning it seemed like we had a lot of time to cover this ground. Here

we are almost at the end of our hour. This has all been fascinating, but there are a lot of things we haven't even touched on yet.

I'd like to ask how we are going to achieve some satisfactory level of consumer understanding broadly and generally about this whole business.

We have been talking about this as our property that should be incorporated in this or that product. We need to broadly and generally understand this.

Miss Mulligan I believe used a phrase that really hit a hot button on me. She talked about the intelligibility of consumer disclosures. This is something that regulators grapple with and are enormously frustrated by all the time.

Talking about specific products that are in the process of being introduced, I wonder how producers of those products are addressing the privacy properties of their product in terms of disclosures, how this can be effectively addressed so that it can be broadly understood, and what if any enforceability capabilities need to be introduced to make sure that people are given an appropriate level of accurate understanding of what it is that they're using. That's a broad, general topic to anyone who would like to take it on.

MS. MULLIGAN: We did a brief examination of disclosure statements of a number of different companies that are in our testimony. We looked at CyberCoin, E-Money, DigiCash, First Virtual, Mondex, Net Cash, and Net Bill.

And just on the disclosure point, I think the only one that really made an attempt to make a complete disclosure to consumers not just about what information would be available at the end points, but also how information captured by the system would be used was Net Bill. They did a fairly thorough job. I wouldn't rate them an A plus, but they really made a stab at communicating kind of the whole package, of how we capture information.

It's not an easy task. A lot of the discussion that had gone on at the Federal Trade Commission about how to provide notice. Trustee, which is a self-regulatory model, made effort to give people just kind of simple branding so that people can understand how information flows. A common vocabulary for expressing data practices is really needed if it's going to become something that consumers can look at like an FDA. That probably is not a good example, like a label to figure out the calories or the content.

We need something akin to model type disclosures and vocabulary. The Smart Card Forum is working with their members to develop those types of disclosure statements. I think it's something that has to be done in conjunction with consumers.

I certainly know as a policy person that I don't very often speak in a language that is intelligible to consumers. I think there is a role for people who have an expertise in the data practices area because, it is a really obscure topic to many,

many consumers.

MS. GRANT: Just look at the print information that you get when you get your credit card at the explanation of your rights and responsibilities. And that's an example of how not to do it I think. It really needs to be in plain English up front.

I think that there is a role of government perhaps in devising some definitions for things so that people are all calling the same thing the same thing, otherwise I think it will be very confusing for consumers to know when different terms are thrown around exactly what they mean.

MS. CULNAN: I wanted to add to that common definition and perhaps even a role for common messages. If you repeat the same message over and over again from different entities, consumers will be more likely to understand.

And if it is possible to work together in the mode that the Consumer Federation of America led the Consumer Literacy Consortium. There, you have a wide range of entities working together to develop common messages which can be repeated and build an understanding in the mind of consumers. I think that might be very helpful and a good role for government to lead.

MS. SULLIVAN: I think the Commerce Department has been trying to work with industry to develop pieces like this. I think that banking regulators that have an interest in working with industry on this, should avoid the truth-in-lending disclosures that you just talked about that have been the result of years and years of regulations and laws that really don't serve the purpose that they meant to serve.

I think that one of the terrific things that is going on right now is that we're not repeating the errors that we made before in developing other products and services. So any kind of educational aspects that the industry and the regulators could work on I think would be terrific.

MR. LUDWIG: Governor Kelley. Do you have any other questions?

GOVERNOR KELLEY: I think that's very helpful.

MR. LUDWIG: Anyone else?

MR. GUYNN: Can we take Mike's line of questioning one step further. I'm scared. Marc, you were talking about the work that's been done, analytical work to see what customers want.

Has anybody done any legitimate good research on what customers really know and understand about privacy issues related to products?

Has anybody taken a product or a series of products and talked to users to ascertain whether or not the kind of disclosure that people are trying to do and we all agree is really important is really taken? Do people have any sense about what's happening to the data?

MS. CULNAN: There are some real big gaps in the survey research that's been done. One of the things you learn from doing surveys is every survey raises new questions that you

didn't. But two questions that have never been asked and I think need to be asked is one, what do people think is going on with their information? What is the level of understanding?

And then the second question is do you care? If people really don't care, then what's all the fuss about? And if people do care, they say they're concerned about their privacy. They say they've lost control.

Do specific practices associated with specific products, cause problems for people? So if someone would put up the money to do one of these surveys, which tend to be fairly expensive, and ask some of these questions, it would be enormously helpful in moving the discussion forward.

MR. GUYNN: This argument is terribly important on both sides of the table to have some sense about what people really know about what's happening because I don't think we do.

MS. CULNAN: Right. These lobby surveys have been funded by industry and they maybe are afraid to get the answer to the question.

MR. LUDWIG: Yes. One of the keys to all of that is the survey. It depends on how you ask the question. How much does the consumer know when he or she says, “I don't care.” The consumer has to be informed as to what the consequences of not caring are.

MR. ROTENBERG: I'm a little bit skeptical of policies that rely on extensive consumer education. And I say this in part looking at the current debate over debt card liability and the confusion in many consumers' minds.

Equally important to consumer education is also business education. If consumers really do want these services for anonymity and to protect privacy, it isn't always the case that they emerge quickly in the marketplace, particularly where there are some macro issues related to the development of they payment systems.

I hope part of what comes out of this session is the expectation that businesses will be more responsive in the development of those services and the creation of these policies to protect privacy.

MR. LUDWIG: With that, let me call this first panel to a conclusion. Thank you, presenters, for really an excellent set of presentations and comments. Since I must leave this hearing, I did want to take one moment before I turn the gavel over to Chairman Pitofsky to thank publicly the staffs of all the agencies for doing a wonderful job in this public hearing and the prior public hearing. I know they've worked enormously hard. I know my own staff has done a splendid job. I just wanted to express my personal thanks and turn the gavel over to Chairman Pitofsky after the break.

PANEL ON SECURITY ISSUES

Demonstration: Thomas Smedinghoff, Esq., McBride, Baker & Coles
Panelists:
Catherine A. Allen, Chief Executive Officer, Banking Industry Technology Secretariat
Marcy Creque, Midwest Region Volunteer Director, American Association of Retired Persons (AARP)
Shabbir J. Safdar, Owners Telecommunications Watch Paul Lampru, Strategic Marketing, VeriFone
Elliott C. McEntee, President and Chief Executive Officer, National Automated Clearing House Association (NACHA)
Michelle Meier, Counsel for Government Affairs, Consumers Union
Wayne Miller, Vice President of Information Services, AT&T Family Federal Credit Union
Russell B. Stevensen, Jr., General Counsel, CyberCash, Inc.
Peter Toren, Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice

CHAIRMAN PITOFSKY: Moving on now to our second panel. Jim Kamihachi will be sitting in for Gene Ludwig on behalf of the Comptroller's Office.

I'd like to introduce the second panel which will discuss security issues that are relevant to electronic payments including the consumer concerns about unauthorized use and liability, encryption, and forms of authenticating a payment or a user such as signatures.

Our panelists are Catherine Allen, Chief Executive Officer, Banking Industry Technology Secretariat; Marcy Creque, Midwest Region Volunteer Coordinator, American Association of Retired Persons; Alan Davidson was to be here but cannot, and substituting for Alan Davidson is Shabbir Safdar of the Owners Telecommunications Watch; Paul Lampru is the strategic marketing at VeriFone; Elliott C. McEntee, President and Chief Executive Officer, National Automated Clearing House Association; Michelle Meier, Counsel for Government Affairs, Consumers Union; Wayne Miller, Vice President of Information Services, AT&T Family Federal Credit Union, on behalf of the National Association of Federal Credit Unions; Thomas Smedinghoff, of McBride, Baker & Coles; Russ Stevenson, General Counsel of CyberCash; Peter Toren, Trial Attorney, Computer Crime and Intellectual Property Section of the Department of Justice.

I'd like to thank all of you for being here today. I'd like to start off the panel on security issues with a presentation on digital signatures by Tom Smedinghoff of McBride Baker.

MR. SMEDINGHOFF: I've been asked to provide a basic overview of digital signatures, how they work, and the legal issues that they raise. I've been told I've got 15 minutes to do it so I'm going to do it at a relatively high level. And I

apologize to any of the technology people here who might feel that I missed some of the finer points.

The best way to start out was to look at the legal requirements that you had for most forms of electronic transactions such as electronic contracting that might occur over the Internet. And I've boiled those down to four basic issues which I call authenticity, integrity, nonrepudiation, and legal formalities.

By message and authenticity I mean who really sent the message and, in some cases, do they have the authority to act on behalf of the entity that they're purporting to act on behalf of. If it's a payment order received by the bank, the bank needs to know who sent it and if they had the authority. If it's a document of a contractual nature, we need to know who we're dealing with on the other end of the transaction.

Second, we need to look at issues of message integrity which basically boil down to is the message complete and can we have some level of assurance that it has not been altered either in terms of alterings that might occur during the communication of the message or alteration that might occur at either end once the message is stored on the computer of the sender or the recipient. We need some assurance that we've got the complete message and that it has not been altered.

Third and really flows from the first two. If we're going to commit resources, change our position, send money, deliver product, whatever it is in reliance on an electronic message, we generally need some assurance that the sender of the message cannot repudiate the message and either falsely deny that he or she sent it or falsely deny the contents of the message.

And finally, in many cases we have to deal with legal formalities, typically writing and signature requirements, for example, for the statute of frauds that applies in a contractual situation.

And we need some assurance that we have been able to satisfy those requirements. If we look at traditional paper-based commerce, there are a lot of ways that almost unconsciously we use these requirements. They may not be particularly secure, but we've trusted them for so many years we tend to rely on them. Things like the use of paper where the message is bound to the paper and cannot be separated.

Colored backgrounds, for example, on a check, letterhead, ink on paper, handwritten signatures, sending messages through sealed envelopes through a trusted entity like the U.S. Postal Service. All of these things rightly or wrongly help us to feel comfortable when we deal with a paper-based commercial transaction.

When we move to the Internet in electronic commerce, we don't have these basic indicia over liability so we need a substitute. And that substitute is information security. With information security we are protecting the message because we

recognize that when we use a public network like the Internet, we cannot protect the medium itself.

The important thing to recognize with respect to information security is that not only does it have a technical component in terms of how it works but it also has a very significant legal component.

This was first recognized in the Uniform Commercial Code Article 4A dealing with wire transfers where information security procedures in effect replaced the signature as the authenticating device for payment orders sent electronically.

The primary focus from the perspective of Internet transactions when we talk about information security is the concept of a digital signature. So what I really want to focus on here is three issues with respect to digital signatures.

First, what are they? Second, how do they work? And then third and briefly, what are the legal issues that they raise?

I have always thought when talking about what a digital signature is that it's helpful to start by talking about what it is not just for clarification purposes. A digital signature is not a digitized copy of your handwritten signature like might be created when you sign one of those little credit card pads at a department store.

Likewise, it is not your name typed at the end of an E-mail message, even though that's transmitted digitally. And third, it's not a PIN number like you might use in connection with an ATM card.

What a digital signature is actually boils down to a fairly technical definition. But I've distilled three basic elements. First, a digital signature involves a transformation of the message itself. That's important because it links the signature to the message.

Second, it uses public key encryption to accomplish this. Finally, it does it in such a way that the recipient of the message can verify the authenticity and integrity of the message. Who was it from and is it complete or has it been altered?

What does a digital signature look like? Here's an example of a plain text message which you can see in right at the top of the slide where somebody is purporting to enter into a contractual transaction.

The bottom of the message highlighted in yellow is the digital signature. Two things that ought to be noticed here. First of all is the fact that that signature is total gibberish. It means nothing when you look at it and you can't tell whether that message is authentic by looking at it. The signature is created by software and it's interpreted by software.

Second, you can read the message itself. When we digitally sign a message we are not protecting the confidentiality of the message. That's a wholly different and separate issue. Okay.

Let's talk briefly about encryption. I'm sure everybody is basically familiar with the concept of encryption, the process of

disguising a message in order to hide its substance.

It's important to focus on the fact that there are two different types of encryption, symmetric encryption and asymmetric or public key encryption. Symmetric encryption has been around literally for thousands of years. The Greeks and the Romans apparently used some form of it. The Germans had their enigma machine in World War II. And there's the Captain Midnight decoder rings.

Asymmetric public key encryption was basically developed in 1976. It involves the use of two separate keys. The importance of distinguishing the two is to recognize that traditional symmetric encryption is what we use for confidentiality, and public key encryption is what we use for digital signatures.

A little bit more on public key encryption. First of all, the keys that we're talking about are not really keys; they're basically large prime numbers. They're generated typically by the person digitally signing a message.

They would use one of these key pairs using software or a hardware device. You generate two keys: one is called a public key and one is called a private key. The private key you keep confidential. That is what you use to digitally sign a message. The public key is disclosed to anyone with whom you might want to communicate the message, any one of your trading partners, for example.

And these keys have a couple of very important characteristics. They are mathematically related. They come in a pair and each pair is unique. There's only going to be two particular keys that can form a pair. We cannot have a third.

And second, you can use either key to encrypt a portion of a message, but then you have to use the other key in order to decrypt it. And that is a very important characteristic of public key encryption.

If you think, for example, of two physical metal keys that you'd use in a lock on a door, if we could construct a lock such that one of those two keys could lock the door but then you had to use the other key in order to unlock it, if you had one of those two keys and came up to the door and found it locked, put your key in and you were able to unlock the door, it would get you in the house but it would also tell you something very important.

It would tell you who locked the door; that is, the person who holds the other key. And that's the basis behind the digital signature process is by tying these two keys together and tying the keys to an identity we can tell who sent a message.

Let's look briefly at the process of creating a digital signature. Now this is all going to be done by software. It would be transparent to the user. But it's instructive to see how it works.

If we start at the left-hand end of that slide, the box labeled message, that's our plain text readable message that

says, “Take a thousand dollars out of my account and send it to General Motors”. We take that message and run it through something called a hash function.

A hash function is nothing more than an algorithm that translates the message into a unique in effect a number which we called here a message digest. But the significance of that digest is that it is unique to the message.

If the message changes, the digest changes. If we add a comment, if we change a yes to a no or a thousand to a hundred thousand, the message digest is going to change. So the message digest is like a digital fingerprint of the message.

We then encrypt the message digest using the public key of the signer. The encrypted message digest is in fact the digital signature. That is attached at the bottom of the message which is then sent on to the recipient of the message.

So, the message looks much like the one we just looked at. You have the text and you have the digital signature attached at the bottom.

When the recipient receives the message, the message is received with the digital signature attached, the recipient software is going to do two things. First across the bottom of the slide there, it looks like the lines aren't real clear but there is a line running from digital signature to encryption function, the first thing the recipient software will do is decrypt the digital the digital signature to see if it can determine the contents of that message digest that the sender calculated before it sent the message.

If the recipient can decrypt that message, then we've established authenticity. We know who sent the message. It's the person who holds the private key that matches the public key that we used to decrypt the message.

And then second, across the top of the slide, the recipient software will take the message itself and run it through the same hash function in order to calculate a digital fingerprint of the message as received, which we call message digest number two.

We then compare the digital fingerprint of the message as received, message digest number two, with the digital fingerprint of the message as sent, message digest number one.

If those are the same, we know the contents of the message have not been changed since it was sent by the sender and we've established message integrity. There is one key problem with this whole scheme.

I said a minute ago that when the public key is used to decrypt a digital signature, we know who sent the message. It's the person who holds the matching private key. But who is that? Keys are just numbers and anybody can have a particular number.

How do we relate a number to a person or an entity? Well, the answer to that is we use a trusted third-party known as a certification authority. The job of the certification authority is to identify an individual or an organization or a machine, for

that matter, and associate that identity with a public/private key pair.

And then what the certification authority does is issue a digital certificate in order to accomplish that. A digital certificate basically binds a public key to an identity.

So if I get a message that purports to be from Bill Gates, I would go to a certification authority who has issued a certificate to Bill Gates, get a copy of that certificate, look at the public key that appears in that certificates, and use it to attempt to verify the digital signature that we receive.

These certificates are typically, or at least in theory, going to be published in publicly accessible on-line repositories. In some closed systems they would not necessarily be publicly accessible. But the concept is there would be a database of certificates that you could go to to retrieve that certificate in order to verify a digital signature.

If you have not gone through the process, you can go to the VeriSign Web site. You can actually have your Netscape browser calculate a public/private key key fare for you. You can then use that to apply for a digital certificate from VeriSign. It's a worthwhile exercise to go through to see how this process works and to take a look at the resulting signature.

Now what are the legal issues? I've got one slide here to summarize what could be weeks and weeks of discussion, but I boil it down to three categories of issues.

We need to focus on what are the obligations of the parties to a digitally signed transaction, what is the effect of using a digital signature, and how do we ensure that the certification authority properly identities and goes through the appropriate processes when issuing a certificate?

With respect to the obligations of the parties, there's going to be three parties to every digitally signed communication. There's going to be the person who signs the message, the certification authority that issued the certificate, and the relying party, the recipient who uses that certificate to verify the digital signature.

The sender of the message, the person who signs the message is the person who holds the private key. The key obligation of that person is to keep that private key confidential. If it turns out that private key is compromised, somebody else could send a message masquerading as the individual signer.

This also raises issues about what is the scope of the obligation to keep that private key confidential. It also raises issues in a consumer context in terms of whether we want to apply those same rules to consumers that we might apply to businesses.

When we look at certification authorities we have to ask the question of what is their obligation to properly identify individuals when they issue certificates. And what is their liability if they don't properly do their job?

When we look at the recipient of an electronically digitally

signed message, we have to focus on their obligation to get that certificate and verify that digital signature before they can rely on the message.

What's the effect of a digital signature? Some states are starting to say that a digitally signed message will be given in essence legal presumptions if there is a dispute and we have to go to court.

Basically what the states that have done this are looking at is a rebuttable presumption that the identified signer is in fact the signer of the message.

A rebuttable presumption is that the contents of the message have not been altered, thus shifting the burden to the other party to disprove that, similar to the approach that Article 4A takes with respect to payment orders sent pursuant to a commercially reasonable security procedure. Other states have rejected that approach.

Third is the issue of quality controlled certification authorities. This is a major, major question. Some states have taken the approach that we need to regulate and license certification authorities. We need to require them to post a bond, to be audited, and to go through a variety of procedures and regulations to make sure that they properly identify people with public keys.

Other states are taking a more laisser-faire approach, and others are looking at different alternatives such as accreditation that might be used to accomplish this process.

If we look at the legal infrastructure that's starting to be built with respect to digital signature rules, there is a lot going on. The American Bar Association Electronic Commerce Division, which I chair, issued the digital signature guidelines about a year ago through the Information Security Committee. They have been very influential in focusing this debate.

Those guidelines function much like a restatement of the law in terms of setting forth what the principles ought to be relating to digital signatures. Then, as you can see from this list, there are a few states that are looking at various forms of digital signature legislation.

There was a paper on the table. At the end of that paper is a summary of the current status of all of the enacted and pending state digital signature legislation. As you can see from taking a look at that, at last count there are 39 states that are doing something in this area. Some are focusing generally on electronic signatures, others are focusing on digital signatures, and some are doing the regulatory licensing route.

Other states are taking different approaches. It's a mixed bag right now. The states seem to be pretty much all over the ball park. Where that's going to end up I think is an open issue and the need for uniformity I think is a very, very serious problem there.

And then in this last slide I just summarized Web sites

where further information is available. And with that I will close and turn it over to the next speaker.

CHAIRMAN PITOFSKY: Thank you very much for a truly fascinating presentation. Once again I get the feeling that future shock is right upon us.

Let's turn to our panel of speakers.

MS. ALLEN: BITS is the division or separate entity from the Bankers Roundtable. The Bankers Roundtable is the 125 largest bank holding companies in the U.S.

BITS is, the board of BITS is made up of the ten largest banks. And they represent 70 percent of the deposit assets in the U.S. We also have representatives from the ABA and the IBAA on that board.

The mandate for BITS came out of concerns in the public and also concerns on behalf of the financial services community about security and privacy. One of the research pieces I like to quote is Yankelovich and Associates.

They do it from year to year, along with their Cybercitizen survey and their regular consumer surveys. From last year to this year a significant shift in concerns on behalf of consumers about security and privacy. They in fact put security before privacy.

What they mean by that is who has access to their bank accounts or their credit card numbers and also what's being done with the information that they've providing. What's significant in the research is that women are more concerned than men.

Eighty-five percent of the regular on-line users that are women versus 50 perfect of men say they will not shop or bank on-line until they feel that these safeguards are in place.

It's part of that that has led to the initiatives around BITS. The mandate for BITS is to promote the security and safety and soundness of the payments and financial services delivery systems.

So we're looking at both the payment component as well as the broader definition of electronic commerce and where payments and transfer of information takes place. We're organized around a number of initiatives.

The six initiatives deal with establishment of standards, irreparable and open environment standards and specifications in the technology world, looking at a larger group of consumers to be able to access the system. Perhaps the development of an Acceptance Mark or a Privacy Mark will ensure that consumers understand that the system that they're working over is safe and sound.

I'll talk in a little more detail about that. We have an advisory group which is meeting right now in the Washington Sheraton. The designees from the chairman are their senior executives that they listen to.

That forum is my kitchen cabinet. We have working groups around deliverables by September and we have five deliverables.

For September in the privacy area, we not only are working with the CBA and the ABA on developing industry-wide adoption of guidelines on privacy, we are going to step further to how you would implement and enforce this.

We had a discussion this morning about this on guidelines for the industry in terms of what business practices need to change and how it might be enforced. I think that will be a continuous dialogue with the government on this.

A second deliverable is in the standards area. It is bringing together various parties that have differences in the home banking, Internet, and Smart Card arena, where payments and financial services are involved and tried to make those an open environment and interoperable and secure.

A third effort is in what we call industry review where we are looking at the different payment mechanisms, different payment entities, and rationalizing what they're doing so that there is a concerted effort and strategy on behalf of the financial services industry.

The last two have the most perhaps interest to you are two meta-architecture projects. We're taking a methodology that was developed for the telecommunications. and systems integration world and applying it to the payments infrastructure. So we have a process on developing a meta architecture of the existing payment system which will allow us to understand the roles, rules, regulations, and potential security breaches.

That's everything from cash and checks all the way through to ACH and chips. Then we have a de novo meta architecture group which you're seeing if we didn't have to worry about the legacy systems. Or, if we were coming at this as a software provider or a nonbank, how would we deliver an electronic commerce framework?

Once we have this meta architecture design, we are then going to bring in some security companies, one to design and one to detect. Most likely it will be our national laboratories like Sandia or Los Alamos that will help us see where the potential breaches may occur in the existing systems and where they may occur.

We're being inclusive in this. We have a series of industry forums where there are government people. Jim is actually coming out to our August meeting in Santa Fe where we're focusing on the consumer and business issues. Again, we are going to the customer and what are their concerns about trust, security, and privacy. Then, how do we implement that into the design of the de novo meta architecture.

Certainly on the security arena, I think that we will have your interest and involvement. Some of the agencies have already been participating in our industry forums. I've given you some materials to tell you about that.

Two specific things are of interest. One is that behind the privacy implementation was the feeling on the part of the banks and financial services community that we have to take the high

road in the leadership in this arena, that it's important to our customers.

Banks have a long-standing tradition of keeping information private. If we can use not only how we have done that, but also how we have worked with the government in that, that might be a model for other industries to follow.

The second thing is in meta architecture and security. We all know that all securities are breachable. The issue is what are the business tradeoffs and what are the tradeoffs for consumers.

That's where dialogue with the government and the consumer groups and the consumer marketplace is necessary.

Let me in conclusion restate how important security, privacy, safety, and soundness are to the financial services community. That's the reason BITS was developed. We were funded in November, and I just took over as CEO on April 15. So we're up and running, and it's all focused on safety, soundness, and security for financial services.

Secondly, it's critical that we understand the customer marketplace and customer needs. The users, the financial services community, and the government are really laying out the business criteria for the technology players to follow rather than the other way around.

The technology players are saying that this is what we have to use and here's how you'll use it. So I think having this sense of security and soundness is critically important. We need to communicate that to the technology providers and the new entrants to the new industry.

I invite you to participate in the industry forums, and I look forward to other dialogues. And we do have some follow-up meetings.

We're meeting with Governor Kelley later this month, and Attorney General Janet Reno has asked to meet with a number of our CEOs on security. So I'll be glad to share that information with you.

CHAIRMAN PITOFSKY: Thank you very much.

Miss Creque, could you give us reviews from the point of view of AARP?

MS. CREQUE: Mr. Chairman and members of the Task Force, AARP again appreciates the opportunity to present our views on the issues of safety and soundness and the protection of privacy regarding emerging electronic money technology.

My name is Marcy Creque, and I'm a regional volunteer director for AARP's midwest region. Emerging electronic payment technologies promise many benefits, but also may make consumers vulnerable to financial fraud and abuse.

Safety and privacy issues for financial institutions and consumers are not always identical. For example, banks and other institutions may be concerned about such issues as digital signatures, encryption, and securing equipment and devices from

theft and vandalism.

Consumers place more emphasis on the soundness of issuing institutions or entities that control the means of accessing accounts and services and conducting transactions.

Some areas of mutual concern because of the threat of shared loss, such as the theft or loss of transaction cards, personal identification numbers, and computer access codes.

My remarks focus on a few of these areas most important to consumers. The confidence of older persons in the safety, security, and financial soundness of electronic money affects their willingness to utilize these new technologies.

AARP's position on safety and soundness is derived from the fundamental need to assure that retirement savings and other financial assets often accumulated over a lifetime are available when needed.

While AARP agrees that many benefits can be derived from new innovations, a Congressional Budget Office report notes that the regulatory framework for emerging electronic payment system is uncertain.

For example, a recent legal opinion issued by the Federal Deposit Insurance Corporation found that while a stored value card could be designed in such a way that it would be covered by Federal Deposit Insurance, no existing stored value system qualified for FEIC coverage.

In contrast, a credit balance on a credit card when the bank issuing the card fails is deemed to be an insured deposit and is covered by insurance. On-line script or stored value cards can be issued by non-depository and depository institutions, but only depository institutions are covered by deposit insurance.

Electronic money issued by nonbanks, however, would not be insured even if distributed or sold by banks. The Federal Reserve says stored value balances issued by depository institutions will be treated as transaction accounts subject to reserve requirements.

It lacks authority regarding balances issued by non-depository institutions. Finally, the Federal Reserve has not indicated whether reserve requirements would apply to on-line script.

Also, issuers or financial backer failure or even fraud are possible. In fact consumers have already suffered losses due to prepaid phone cards issued by fraudulent companies.

Operational failure or insolvency of a key issuer could create a loss of confidence in electronic money and lead to additional insolvencies and perhaps impact the ability of banks to meet their interbank payments.

Although insurance coverage to closure is required on some products by regulatory agencies, actions on available instructions lack enforcement. AARP agrees with the CBO's report which concluded that clarification of some of the legal ambiguities regarding safety and soundness would aid acceptance

of electronic money transfers by merchants and consumers.

Disclosures about deposit insurance coverage would be especially helpful. However, those products offered by non-depository institutions would remain a problem.

State laws governing check and money transmissions by nonbanks offer only partial protection to consumers. Some 45 states have sale of checks, money transmission licensing laws.

But only half of these laws specifically apply to the transmission of funds by these means. In addition, these laws are unlikely to apply to non-financial institutions engaged in Internet commerce since they require a presence in that particular state.

Models should be developed and tested to determine suitability of national or nationally approved standards. Closely related to these financial safety and soundness concerns are a host of privacy issues.

Among these are the confidentiality of the individual's financial records. Gaps in legal protections resulting from differing state and federal laws, unauthorized disclosures, and ownership of data that is either transmitted or stored electronically for the purpose of initiating, inducting, verifying, or recording financial transactions.

Different payment methods afford different levels of privacy. According to the CBO's report, the Right to Privacy Act would not apply to products issued by non-financial institutions. Neither are state laws likely to apply.

Most of the law cited above apply primarily to government rather than private sector use of information. A March 1997 report to Congress states that fraud-related identity of theft appears to be a growing risk for consumers and financial institutions.

The relatively easy access to personal information may expand that risk. Social security numbers and the so-called header information are easily available from reference services over the Internet.

Providers place few if any restrictions on access or intended use of the information. Because electronic money technology can generate and store a great deal of information about individual payments and assets, the potential gaps in legal protections are of great concern to consumers.

Information obtained through the use of electronic money products may be disclosed without their consent and used for fraudulent purposes or in a manner adverse to their interest.

The security of on-line transmission is also a concern as more older persons purchase home computers and use them for banking and financial management services. Older persons are particularly concerned about unauthorized disclosure because they are frequently the victims of financial fraud.

AARP agrees with most of the principles on privacy developed by the task force study of the United States Advisory Counsel on

the National Information Infrastructure. A list of those guidelines endorsed by AARP can be found in the long version of my remarks.

We look forward to working with the Task Force in developing solutions to the electronic money issues of safety and soundness and the protection of privacy.

CHAIRMAN PITOFSKY: Thank you for a very useful review of the different levels of security in different forms of payment.

As I mentioned earlier, Mr. Davidson is not here. Mr. Safdar of the Voters Telecommunications Watch is substituting.

MR. SAFDAR: I was mentioning the goal of the group to a friend and mentioned the theme, The Future of Money. She asked me if they're going to redesign the hundred dollar bill again. I'm glad we won't be talking about that today.

I want to reiterate a theme voiced by the previous speaker which I thought was very good which is consumer confidence. Consumer confidence is a critical element to any electronic payment system. It's a concern across the demographic spectrum.

In particular we have excellent examples of systems that did electronic communication that had fatal flaws in their openness, which point us to one of the features we should look for in future electronic payment systems.

It is not unusual that we should find this level of concern among consumers in an era where a bug in Netscape or any other Internet program makes above-the-fold news in the "New York Times."

In particular, consumer confidence comes with a number of factors. But initially it comes from an assurance that the system has integrity. The place that we tend to look for that is to the academic community into peer review.

When we look at algorithms such as the data encryption standard which is now over 20 years old, we see that in the last several years the cryptography community has attained a comfort level with that standard being secure.

The same thing goes through for other algorithms that are involved in communications and payments. As Mr. Chaum can attest, it is in fact very, very difficult to design a secure protocol or a secure algorithm.

It is very, very easy, of course, to design one that looks secure but is not. And the key to this is openness and peer review. An excellent example of this would be the protocols that went into the administration's clipper chip program several years ago.

Both the algorithm and the protocols were kept secret for security reasons. We were given the highest assurances that that was highly secure.

A scientist at the time at Bell Labs, Dr. Matt Blaze, proved that the algorithms were not secure, or at least the protocols were not secure. And the algorithm skip jack which is coming to light now as we look at new algorithms to replace those is going

to become public and will undergo the same scrutiny.

I think that what this experience teaches us is that consumer confidence, and, more importantly technical confidence in the system, comes from openness and peer review.

In any system, the time has come and gone for proprietary systems with either propriety algorithms or protocols to be an element of that. So I would urge you in looking at such systems to mark that.

It has a very, very important aspect and affects consumer confidence and the very security of the system itself as being a replacement.

CHAIRMAN PITOFSKY: Thank you.

Our next speaker, Mr. Lampru?

MR. LAMPRU: It's my privilege to be here today to offer VeriFone's perspective regarding Internet security for financial and non-financial payment systems.

VeriFone is a global firm with headquarters in Redwood City, California. In 1997 our revenues exceeded $500 million. We do business in over a hundred countries and employ about 3,000 people.

Most of you know us although not by name but by the small gray boxes through which retailers swipe your credit card.

We have more than five million of those gray boxes installed. Recently Hewlett Packard completed the acquisition of VeriFone in a stock swap valued at roughly 1.1 billion.

When Master Card and Visa agreed on the Public Key Cryptology and X509 Version Three Certificates as a foundation for the SET protocol, it was a major milestone in the development of the Internet as a viable communications infrastructure for business.

The Master Card and Visa SET protocol is strategically important for Internet commerce for a number of reasons. First, SET is a global credit card payment system that depends on Public Key Cryptology. It requires consumers eventually to obtain Public Key Certificates.

The SET protocol is a powerful catalyst that is accelerating the introduction of chip card reader/writers into consumers' homes. So the Private Key, associated with one's credit card number, can be stored on a transportable and not replicatable token such as a chip card.

Currently a number of groups like the PC/SC working group, Personal Computer/Smart Card working group, are in the process of defining protocols to enable chip card systems to interact with personal computers as well as network computers.

The work group identified a specific set of objectives and aimed at defining a comprehensive and flexible solution for integrating ICCs, integrated chip cards, with the PC and documenting these efforts in a specification.

HP as well as a number of other keyboard manufacturers recently have announced that chip card reader/writers will be

embedded in PC keyboards. HP's announcement says those will begin shipping in October of this year.

Second, Master Card and Visa are expected to begin marketing initiatives to educate the public on how individuals will use cryptology and certificates to make purchases over the Internet.

In addition, a number of publications are beginning the education process for those readers. Most recently a very good write-up was in Byte magazine in the June issue.

Third, the cost of Public Key infrastructure needed to support secure financial transactions over the Internet is being embedded in consumer Internet-based products systems.

This suggests that consumers will be paying for a large portion of the cost of this infrastructure. If those chip card reader/writers are embedded in the keyboard, that will become just like a floppy disk drive that we know today though the consumer is sort of paying for it.

If this happens, it should improve the business case and accelerate the integration of chip card payment systems into the virtual world as well as into the physical world.

There is a distinct possibility, not a technical hurdle, that would allow Internet-based payment systems to come back down to countertop where we now have magnetic stripe technology. Those would be chip card reader/writers connected to the Internet to allow the haves and the have-nots to use the same terminal for a payment. It might be check, credit, debit, cash.

Fourth, the SET protocol infrastructure can lay a foundation where the Public Key infrastructure that could be used for financial but yet non-financial transactions.

For example, the National Association of State Information Resource Executives (NASIRE), the National Association for State Purchasing Officials, and the National Association for State Comptrollers are seeking creative proposals now from industry to establish accreditation standards for certificate authorities that issue Public Key Certificates that can be used to generate digital signatures that would be legally binding in a court of law.

NASIRE is taking the lead on this issue to avoid each state developing its own set of accreditation procedures, thus slowing down the process for cross-certificate and accreditation necessary for national and international electronic commerce.

I'd like to append that the potential of the Internet is too important for government to monitor commercial developments, wait for inequities before using its influence.

The federal government can and is developing a national strategy that does not curtail commercial innovation, but balances the potential benefits between the public's interest and the private enterprise profit potential.

Such a strategy should be based on a vision or an optimism that points our society toward the highest and best use of this new communications infrastructure.

If the Internet is the driving force behind this shift into the information age, then focusing on the following four key elements might help government harness the Internet and lead to the formation of a national strategy or add to one.

Public Key Cryptology, one. Number two, an open Public Key Certification authority infrastructure. Individual control, that is, in privacy of personal information in commercial databases. And chip card technology.

A very important point that was made in the last session was to enable consumers or get consumers to implement the privacy principles.

Number one, the information could be in the hands of the consumer in a chip card. Number two, it was said that it could be in the hands of a trusted third-party.

I would like to add to that list and suggest where there are advantages and disadvantages of each of those. A third option might be a consumer control over information in the hands of trusted third-parties.

So the combination of both of those to take the advantages of both and try to negate some of the negatives. That I believe can be done with an open Public Key Certification infrastructure.

CHAIRMAN PITOFSKY: Thank you.

We turn now to Miss Meier. We'd be happy to hear Consumer Union's views on some of these issues.

MS. MEIER: Consumers Union is the publisher of Consumer Reports magazine. We also have an office in Washington where I am located.

I have been working in the Washington office primarily on banking and credit issues for many years. I am here today representing both Consumers Union and also Consumer Federation of America and U.S. PERG. We'll be submitting fuller testimony in writing hopefully in August when we have a break.

Before it gets lost in the shuffle, I want to make it very clear our position on the question of self-regulation versus at least some level of legal protection, i.e., government regulation in this area of security.

We think it is very, very wrong, misguided to rely exclusively on industry self-regulation in this area. It's too critical. We are talking about consumers' dollars at stake.

When we are talking about access to checking accounts where people have stored their savings, the question of security is of utmost importance to consumers, individual households, and families.

We must be sure that there are laws in the book that address the question of who is liable when someone without authority gets their hands on that money.

We certainly appreciate the need and the benefit of consumer education. That certainly has an important role here. But disclosure has some role here.

Earlier I listened to the first panel make a number of

disparaging remarks about some of the consumer protection disclosure laws. I had to agree with some of the problems with those laws, but need to point out that if the industry is saying no regulation and putting all its eggs in the disclosure basket, then we need to be real about the limitations of disclosure.

We don't want to come back here in ten years and say these disclosures are so complicated we don't understand them. They're overwhelming to the consumer. The truth is too much disclosure can be overwhelming and disclosure is not the appropriate protection in some circumstances.

What is the appropriate protection? It's substantive protection, liability rules that clearly establish that the consumer won't bear liability when third-parties wrongfully access the account.

Again, the stakes are high. We're talking about people's money. Unfortunately a recent phenomenon that has surprised me personally is a good example of why we can't totally depend on the industry's own self-interest in developing secure systems. I'll get to that point in a minute.

Thirdly, legal protections and government regulation are important because consumers simply can't keep up with all the technological changes to make informed choices.

My mind is boggling listening to some of these more technical presentations today. Very interesting, but as an individual average consumer I don't want to have to understand all that as I go about my daily business making purchases.

Okay. The example of recent market phenomenon that again has very much surprised me and driven home the point to me that we can't totally depend on the industry's own self-interest in developing secure systems is the off-line debit card.

I must admit and claim mia culpa on being a little slow to catch on to this. But for the last few months, I have heard my colleagues in the consumer community and elsewhere say, “Hey, did you know that banks are issuing ATM cards that don't require a PIN?”

And I said, “Oh, that's of some concern.” But I was busy on the Hill doing many things. In preparation for today, I have looked through my files and noticed that there has been a number of news stories of consumers who have had their checking accounts totally depleted with these new on-line debit cards.

They look like your old regular ATM card piece of plastic, but apparently they have been sent to consumers in the millions as replacements for the old debit cards and they allow access to your money in your checking account without a PIN.

Now where is the security there? There is very, very little security there. The consequences are apparently bearing some fruit. We are starting to hear stories from individual consumers who with the PIN ATM system lost money.

We are now beginning to hear stories of consumers who are losing money. Only this Sunday, the "New York Times" had a

feature piece on these new cards and presented the scenario where a small business person in New York did lose money.

He is quoted saying, “I eventually got my money back but it wasn't easy. While Bank of America was investigating the theft, I was totally out of that money. That was about two weeks. They eventually had to give me $500 so I could live. They gave me another debit card and I leave it in my house.”

There was a story even earlier. It was a column by a person who I have not spoken with but he's described here as a principal in a consulting business in Massachusetts who relayed his experience with an off-line debit card. This one I thought was very interesting and relevant today because it goes to the question of whether consumers even know that they're carrying these high-risk cards.

Before I get to this, just so you know the stress he was under, his checking account balance up through his $5,000 line of credit, overdraft line of credit was wiped out.

He writes, “I immediately called the bank's customer service line. Calmly, as if it happened all the time, a representative told me to report the fraud to the police and then go to our local bank office, close our checking account, open another one, get new bank cards and change our PIN which provided security for our transactions.”

Security for some bank transactions it seemed but not for others. We were beginning to realize that somehow without our request or permission our snug ATM card which required entry of our PIN for any transactions at our bank had also doubled as a wide-open debit card.

So, this is the consumer who it says later in the article had gotten a new card assuming it was just an updated version of the PIN-related ATM card that they were used to. And only through this bad experience learned that they were carrying a card that didn't even require the PIN.

Now, this is highly coincidental to me. But as I was going through my mail two days ago, I came across promotional literature from my bank. Somewhat unusual, I opened it and found that I was being encouraged to use my ATM card, which in this literature was described as yes, an ATM card, but also a check card and that I could use it at thousands of retail establishments across the country.

I came to realize after thinking about it for a few minutes I was holding one of these cards and I didn't know it. I had been using that card for several months at ATM locations using a PIN number just like I'd been in the past.

I have had an open wallet for many months, but I did not know the kind of risk that my behavior might suggest. Of course, I didn't even know what was going on.

So in conclusion, there are many more things I could say. But I think the notion of self-regulation exclusively will expose consumers to the kinds of liabilities and financial risks that

our culture has simply not found acceptable historically.

CHAIRMAN PITOFSKY: Thank you very much. The nub of the issue is the one that you raise, self-regulation versus government regulation. I'm sure we'll come back to it in our later discussion.

Mr. McEntee, would you come on next?

MR. McENTEE: I would like to thank the Consumer Electronic Payments Task Force for the opportunity to speak on behalf of the National Automated Clearinghouse Association.

NACA represents 13,000 commercial banks, savings and loans, and credit unions. Today I would like to share with you NACA's views on the future of electronic money, consumer protection and privacy, data security and trust, and some of the initiatives that the banking industry is pursuing in these areas. And I will attempt to do that all within five minutes.

For the foreseeable future, traditional payment systems such as the Automated Clearinghouse Network, debit and credit card networks will be the primary vehicles for clearing and sending electronic payments initiated through Smart Cards, stored value cards, and the Internet.

For example, today well over 95 percent of all consumer purchases made over the Internet are being paid by credit card. At this stage virtually all business-to-business transactions initiated through the Internet are being cleared by check or through the ACA's network.

Stored value cards now in testing are cleared and settled through existing debit and credit card networks. Finally, some of the low dollar Internet payment systems being developed, so-called electronic coins such as CyberCash, are using traditional networks for settling the transactions between a consumer's bank and the merchant's bank.

I expect the situation to continue for some time because traditional electronic payment systems which process over 20 billion transactions a year are well understood by consumers, businesses, and banks and they are supported by mature infrastructure.

These systems also offer robust protections and risk management through existing laws, regulations, and operating rules. When considering evolving payment systems, it's important to assess the adequacy of existing protection. This is particularly true when evolving systems rely on traditional networks for clearing and settling the payments, thereby bringing existing protections into play.

Current consumer payment protections such as those specified by network or operating rules and federal and state laws, for example, Federal Reserve Regulation E and Regulation Z provide ample protection against harm from unauthorized electronic payments and errors.

Current technology already offers the ability to protect records contained in proprietary networks and the data in

individual electronic transactions.

For example, network data such as banks' customer account records are protected through fire walls. Fire walls protect against unauthorized access. Individual transactions are protected through encryption which codes the message in a form that can only be decoded by an authorized receiver.

However, neither fire walls nor encryption address the issue of authentication which is necessary when the Internet is used. The solution to authentication is to use digital certificates issued by trusted entities.

We believe that the banking industry will play a major role in issuing digital certificates to their customers in the future. There are many advantages to banks serving as certification authorities.

Since banks are trusted regulated entities, the accounts of consumers and businesses reside at financial institutions which already manage account numbers, PINs, and other identifiers in electronic form.

Finally, a key role of banks is to manage risk borne by themselves and their customers. To validate the role of banks as certification authorities, NACA's Internet counsel is developing a pilot program that will allow banks to exchange digital certificates on behalf of their customers.

The pilot will also allow the buyer and seller to authenticate each other. The pilot represents a critical step in evaluating payment system readiness, define the needs for interoperability, and finally enabling the banking industry to determine a need appropriate infrastructure needs for Internet-based commerce.

With respect to consumer privacy, which is a very important and critical issue, the Banking Industry Technology Secretariet is taking the lead in developing privacy guidelines that I believe all the banking industry electronic payment networks, ACH, debit card, credit card networks will all implement in their operating rules in the foreseeable future.

In conclusion, in order for electronic commerce to grow and thrive with the trust of consumers, businesses, and banks, error resolution, privacy protection, and authentication must all be part of a comprehensive package.

The combination of existing protections plus the initiatives the private sector has underway and the continuing dialogue with the private sector will ensure that this package will be implemented.

CHAIRMAN PITOFSKY: Thank you very much.

Mr. Stevenson.

MR. STEVENSON: CyberCash is in the business of providing technology and services to financial institutions to enable secure financial transactions on the Internet.

Our goal is to provide for the Internet a complete suite of payment mechanisms which are analogs to the payment mechanisms

that we are all familiar with in the three-dimensional world.

I'm going to depart from the remarks that I had prepared for this morning's presentation because most of the points that I made have already been made by others.

And what I propose to do instead is to make a number of general observations. I have learned recently that our friends in the United Kingdom have an expression for certain kinds of observations which they call a BGO or blinding glimpse of the obvious. It has also been said that genius consists in being able to discover and restate the obvious. So I'm going to propose for you this afternoon a number of BGOs which I hope will be found useful.

First of all, security in payment systems is a two-way problem as is its inverse fraud. It is certainly correct that we need to provide adequate security for consumers and other users of payment systems, but financial institutions and providers of payment systems are also subject to fraud.

Usually, because of the way our legal system is structured, that is, with consumer protection in mind, financial institutions and payment system providers end up bearing the brunt of any losses that are sustained in the exercise of the payment system.

And so it is quite clear that businesses, financial institutions that provide payment systems, have substantial incentives to make those payment systems secure. It's necessary to bear that in mind when constructing a body of regulation to deal with those payment systems.

Another observation which is perhaps not quite so obvious is that the very technology that has created the new potential for payment systems that we're discussing today has the capacity for not only making those systems secure but making them in many respects more secure than the three-dimensional analogs of those payment systems that we're all accustomed to.

For example, if I lose my wallet and it has some cash in it, unless the wallet is found by some very honest person I have lost that cash. What you heard this morning from David Chaum, the digital cash system which he's developed has built into it a recovery mechanism so that if I lose my computer or my hard drive fails, I can recover the cash which is stored on the hard drive of my computer.

The same is true for things like credit card authentication. The technology available under the SET protocol will make the use of credit cards in the Internet world more secure if anything than their use in the real world today.

Another BGO is that the payment instruments we are talking about vary widely in their qualities both with respect to privacy and security. We all know that cash is anonymous; a credit card is not.

Cash is insecure in the physical world in the sense that if I lose it or it's stolen, it's gone. Whereas if I use a check and it's stolen I can probably recover any money that's lost if

someone forges that check.

The same qualities are true in these same instruments and their analogs used in the digital world. And it's important again to bear in mind those differences when we are talking about forming policy and regulations to deal with the payment systems.

It is also important with reference to privacy (and on security as well) that we not confuse the privacy implications of payment mechanisms on the Internet with the privacy implications inherent in some transaction.

For example, it doesn't matter what kind of payment instrument I use and how anonymous that might be if I order something which has to be delivered to my home address and therefore have to give the merchant my name and shipping address.

Obviously I'm giving up my privacy there not by virtue of the payment instrument I use. And it's important to keep those differences straight.

Another BGO, if you will, is that in all or almost all anyway payment instruments that we're accustomed to in the 3-D world, there is a trusted party involved, particularly in non-cash payment systems, credit cards, checks, and the like.

We believe at CyberCash, the same will be true on the Internet, that it will not be possible to develop payment systems in which there is not some trusted party involved. Most probably that will continue to be as it is in the 3-D world a financial institution.

Consumers are accustomed to trusting their financial institutions with whom they entrust not only with their money, but a great deal of private information. There's no reason why we shouldn't expect them to do the same on the Internet, assuming that other protections are not absent and so that there is nothing about the Internet transaction which defeats the trust which consumers are accustomed to giving to financial institutions in the 3-D world.

Another thing that must be borne in mind, and I can't say this too often, is that all of the electronic payment systems we are talking about vary substantially in their architecture.

In the 3-D world when you talk about cash, you've got to think about armored cars and safes. When you talk about credit cards, you've got to think about VeriFone point-of-sale terminals and connections to the credit card clearing system maintained by Master Card, Visa, and the other credit card associations. In the 3-D world, the differences between payment -- in the Internet world the differences between payment systems are just as extreme.

Just as you wouldn't regulate a cash transaction in the 3-D world the same way you regulate a credit card transaction or a checking transaction, you can't think about electronic payment systems as all in one lump. You have got to tease them apart and understand that each has differences that have to be borne in mind when we are forming policy and passing regulations.

And finally, I'd like to make a couple of observations which might fall under the heading of “the more things change the more things remain the same.”

The problems we are discussing with respect to fraud, security, and privacy are not new ones just because they have been translated to the electronic world. They do appear with new wrinkles. They have slightly different aspects. Eventually some of them may require some modifications to the existing regulation that applies to them. But just because they're electronic doesn't mean they are new and different.

The other side of that is that we already have in place a legal system and set of rules and regulations which apply to the three-dimensional world that is perfectly capable of dealing with most of the problems that the electronic payment systems handle, at least as they have presented themselves so far.

Fraud is still fraud, whether it's on the Internet or in the three-dimensional world. And we have wire fraud laws and state fraud laws that are perfectly capable with dealing with most kinds of fraud.

I'm not saying that we won't need to modify our systems as we evolve and as new problems become apparent, but let's not rush into creating a whole new legal infrastructure just because we translated payment mechanisms from the three-dimensional world to the electronic world.

CHAIRMAN PITOFSKY: Thank you very much.

Our next speaker is Wayne Miller.

MR. MILLER: On behalf of the National Association of Federal Credit Unions, NAFCU, I would like to thank you for inviting me to be here today and permitting me to voice the concerns and opinions of the nation's federal credit unions.

As member-owned cooperatives, credit unions can offer the perspective of both the consumer member and the financial institution. My name is Wayne Miller, and I'm Vice President of Information Services at AT&T Family Federal Credit Union.

AT&T Family Federal Credit Union has been a leader in technology. Technology is the core ingredient in the credit union's long-range strategic plans. Our members demand alternative delivery methods in providing products and services.

AT&T Family has led the development in implementation of technology such as telephone access, video kiosk, and voice recognition to name a few. The credit union believes that electronic commerce is the next great technology to enter the world's stage.

I have helped develop Internet-based application sensored electronic banking including bill payment, bill presentment, and Web security. Due to their unique membership structure and cooperative nature, credit unions must adapt quickly to innovations in order to satisfy the expectations of their technology-oriented members.

As cooperatives, they willing share their experiences with

other credit unions through trade associations and other networks. The historical credit union focused on efficient service delivery and low-cost operations provided additional incentive to credit unions to move toward cyber systems.

Credit unions are in the best position among financial institutions to extend the benefit of technology to moderate and lower income citizens. Today, at least 850 credit unions have Web sites and many of them offer loan account and account services directly off the Web or through home-base credit union systems.

Fifty percent of federal credit unions also believe that using the Internet to interact with their members will be important to their future success as many credit unions cannot afford brick and mortar to reach their members.

Well over a third of federal credit unions plan to introduce smart and stored value cards within the next few years. Credit unions are aware that there are risks involved in using stored value cards and Internet-based payment systems.

Financial institutions have had to learn to minimize these losses encountered from crime and fraud in traditional delivery systems. Credit unions understand that as the industry makes strides in the technology and the security, the counterfeiters, hackers, and frauds will attempt to advance as well.

This reality will require financial institutions, issuers, and users alike to vigilantly protect the technology and constantly seek creative security solutions.

While credit unions acknowledge the risk and endeavor to protect themselves and their members, we do not believe that the government should attempt to regulate this budding industry.

First, we believe government-regulated security procedures would suppress innovation and limit credit union flexibility.

Second, credit unions believe that any government action at this point would be premature.

Third, financial institutions, issuers, and software companies, the people in the trenches understand more fully what procedures and protections secure transactions require.

Federal regulation of stored value cards and Internet-based payment system security would suppress innovation in the industry.

The private sector has been the primary driver behind the development and use of the security on the Internet for stored value cards. To encourage and continue the creative response to obstacles, these emerging technologies should remain market driven. Moreover, credit unions want the flexibility to decide which card or payment system works best for them and their members.

While we encourage the agencies to solicit information and provide guidance, credit unions feel that government regulation of stored value cards or Internet-based payment systems would be premature at this time.

Where government intervention is necessary, its role should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, and facilitate dispute resolution and not to regulate.

We feel any specific additional regulation would be premature and produce more harm than good. Credit unions merely ask that the agencies permit the technologies to mature with the marketplace before attaching regulations and inadvertently steering the technology.

Credit unions firmly believe that the private sector is in the best position to encourage safe and secure growth of these emerging technologies. Due to its bureaucratic process, the agencies cannot be as responsive to consumer needs and technological innovations as the private industry.

This technology can change dramatically within six months. Private entities have greater incentive for protecting the emerging technologies and consumers' confidence in the technology.

We believe self-regulating initiatives such as the use of SET protocol, digital and digitized signatures, encryption software, and fire walls can adequately protect consumers and financial institutions.

These measures protect consumer identification and ensure legitimacy of the users. Financial institutions also have external auditors whose responsibility is to assess the risk to the institution and implement proper controls.

Moreover, current laws like those protecting privacy and fiduciary responsibility provide further protection to consumers.

In conclusion, credit unions encourage the agencies to solicit information and provide guidelines on how to protect consumers and the financial institutions. We likewise encourage the agencies to solicit information and provide guidelines on how to better secure transaction information.

Credit unions, however, discourage the agencies from implementing any regulation addressing stored value cards and Internet-based payment systems. Instead we encourage the private sector to be vigilant in protecting these technologies from threats and to initiate creative and adaptable solutions to security risks.

CHAIRMAN PITOFSKY: Thank you very much.

Our final speaker is Mr. Peter Toren. Mr. Toren will give us some thoughts from the perspective of the Justice Department.

MR. TOREN: I'm a trial attorney with the computer crime and intellectual property section of the criminal division.

Our concerns or our focus really is a little bit different than what has been discussed by most of the previous speakers. We're most concerned with whether existing laws are adequate to deter fraud in this area, and whether new laws are needed.

Because without sufficient deterrents in this area, the system will not be secure for consumers regardless of the level

of technological security. So we are very concerned about security, but we are kind of focused on a different side of the equation than most of the people here today.

Changes in our society more often than not produce changes in the pattern of criminal activity. No change on the horizon today has a potential for a greater impact than the advent of electronic commerce in its several forms, whether it be stored value cards, debit cards, Internet business transactions, or home banking.

Each of these payment systems, if they become commonplace as I think most of us here today expect that they will, will fundamentally change the way in which Americans transact business and potentially, and I underscore that, potentially make it far easier for consumers to be defrauded and for criminals to get away with their crimes.

Many commentators in this area believe that widespread electronic commerce is probably inevitable. As we all know, it offers real benefits to both consumers and businesses and in many respects is far more efficient than the system that is in place today.

But like any new system it is not without its risks and dangers; consumer fraud of course being only one of them. We have learned from history that as soon as any technology arrives some individuals will attempt to misuse it and abuse it.

For example, the invention of the automobile allowed people to be more mobile than ever before, but also provided bank robbers with a better means of escape than a horse.

Telephones not only allow people to communicate worldwide for both business and pleasure, but unfortunately are often used to bilk citizens and defraud citizens out of their life savings, and of course to interrupt many a family dinner.

In the same way, the identical electronic commerce technology that will save time and money can also be abused probably in many ways that we cannot even imagine here today. But we can make some predictions.

For example, as money enters this brave new world, so does counterfeiting. In fact, for the very first time, the advent of electronic money offers the threat of a perfect counterfeit. Since electronic money is only a string of computer bits, then someone somewhere can make a perfect copy of a stored value and another and another without having to get the right kind of paper and ink, the microfilaments, and the watermarks.

The criminal who learns how to decrypt the stored value card can create for himself an unending stream of money. It is pretty certain that before most Americans will entrust their technology to computer chips they will want to be convinced that this technology is as least as secure as cash and credit cards.

The widespread use of fraudulent stored value cards can also have the effect of undermining consumer confidence even before the system has had a chance to be tested. Further, the lack of

basic information and legal protections in this area discourage the use of stored value cards.

There are currently very few, if any, laws that govern the issuance of stored value cards. It has been suggested before the use of stored value cards will become wide-spread, uniform legal standards governing the issuance and use of store value cards must be enacted.

Despite the novelty of stored value cards, it has been reported that criminals have stolen more than $50 million from consumers and phone companies through the fraudulent sales of stored value cards, and several issuers of stored value cards have gone out of business after selling tens of thousands of worthless stored value cards.

However, for us in the law enforcement, the greatest in this area is that advent of electronic commerce will greatly facility money laundering. While the issue of money laundering is not usually associated with the issue of consumer fraud or security, any system which allows criminals to launder their money more easily makes it less likely that they will be apprehended and punished either for the money laundering or for the underlying criminal activity.

A person in the past who may have been deterred from committing consumer fraud may soon determine that because the possibility of getting caught has been so reduced it has become worth the risk.

Potentially then, this area will attract more criminals and reduce security for all persons involved. Traditionally, as you are well aware, money launderers have deposited their troublesome and bulky cash proceeds into banks or other financial institutions to try and obscure its criminal origins, or they have created phony companies or engaged in sham transactions to launder money.

But these methods usually create paper trails that ultimately can be traced, and have been and are being traced by law enforcement. Further, because of the enactment of new laws and regulations in this area, it has become increasing difficult for criminals to launder their money successfully.

But certain types of electronic payment systems permit virtually anonymous transactions and leave no paper trails. The advent of these systems could permit criminals to successfully launder their proceeds of financial crimes including consumer fraud.

Electronic payments could allow a money launderer who wants to transfer tainted funds to do so without having to take the risk of engaging in personal contact with a potentially suspicious bank employee.

The funds can be transferred anywhere in the world by an automated on-line banking system that can be accessed from the safety of the money launderer's home.

Thus a criminal who might not have otherwise gotten away

with the scheme to defraud consumers because of the difficulty and successfully laundering the criminal proceeds might be able to do so.

Further, some stored value card systems as they are currently designed go further and would permit money launderers to obscure the origins of funds while avoiding the use of financial institutions entirely.

These systems have no central registry of transactions which would allow the transactions to be reconstructed.

The sophisticated money launderer using multiple cards can create an intricate series of transfers that could not be unraveled and that would circumvent almost all existing money laundering laws.

Internet payment systems can similarly permit multiple transactions that could be next to impossible to trace, particularly if unscrupulous merchants cooperate with the criminals.

This would mean, for example, that the chances of apprehending a criminal who successfully billed consumers in fraudulent on-line transactions would be significantly reduced.

In addition to the possibility of making it easier for criminals who engage in consumer fraud to launder their money, electronic commerce may also facilitate the underlying criminal activity. It is likely that swindlers of all kinds from telemarketers to advance fee artists will attempt to take advantage of the anonymity provided by some types of electronic commerce.

To give a single example, if someone today opened up a fake L. L. Bean catalog store, law enforcement would be able to track the perpetrator down through the bank and credit card records of his victims.

But if electronic commerce becomes commonplace, a criminal might open an L. L. Bean on the Internet, a fraudulent one I made add, accepting payment only in digital cash. Not only might these transactions be untraceable, but law enforcement might not be able to determine if the on-line store was in Freeport, Maine, Freeport, Bahamas, or anywhere else in the world.

One step that might go a long way towards eliminating some of these problems would be to implement electronic payment technologies in the way that tracks all transfers or at least all transfers over a certain amount.

Such a system would allow banks or other financial institutions to audit transactions for fraud if not to recreate every transaction. But such a solution raises a fundamental, philosophical issue for our society, the proper balance between anonymity and accountability.

A number of reasons have been propounded for allowing anonymity and communications networks. For example, whistle blowers may want to remain anonymous to avoid retribution. Consumers may wish to obtain information on a product without

ending up on countless mailing lists.

Rape victims or other victims of crime may wish to discuss their experiences without revealing their identities. But criminals, unfortunately, also benefit from anonymity.

Every criminal, of course, wants to avoid getting caught. Anonymous remote communications can help them avoid detection and apprehension. Effective law enforcement requires accountability.

Society must be able to hold individuals who break the law and harm others accountable for their crimes. Anonymous communications and transactions would make it far easier for those who commit fraud against consumers to avoid being prosecuted for their crimes.

The issue of anonymity or accountability is not solely a criminal law issue. It has broader ramifications for our society. For example, if a newspaper prints a libelist story about a person, that individual can sue the newspaper for damages.

The civil suit for damages benefits the victim by helping to restore his reputation. Moreover, it also benefits society by helping to ensure that newspapers report the truth. However, if somebody makes the same libelous claims in an e-mail message over the Internet and routes the message through an anonymous remailer, the defamed person would have no recourse; this despite the potential that the impact of anonymous messages sent over the Internet would be far greater because the contents of such a message could be quickly and widely circulated among all the users of the Internet.

Anonymity in this example prevents accountability. Some commentators have speculated that the often abusive communications encouraged by the anonymity of the Internet may contribute to a weakening of social ties among our citizens.

On the other hand, it has been argued that if we swing the pendulum too far towards accountability, we run the risk of losing some of our civil liberties.

The same electronic commerce system that permits a financial institution to audit for fraud could be modified to keep track of every purchase made by a consumer--every purchase at a grocery store, at a liquor store, at a pharmacy.

Because nearly every transaction could be tracked by the card identification number, for example, consumers could be faced with a prospect of marketers and retailers identifying and tracking their every purchase and transaction.

Existing constitutional and statutory provisions place many restrictions on government access to confidential information. Statutory and common law restricts third-party access to many types of this information.

However, it has been suggested that current legislation which caters to the needs of the past does not address the privacy threats presented by electronic commerce. The principal confidentiality may provide the middle ground between anonymity

and accountability.

In a confidential system, a person's identity is not generally known, but in appropriate circumstances, for example, a person's identity can be determined pursuant to a court order.

Confidentiality permits law enforcement to allow anonymity and inappropriate circumstances but does not permit criminals to obtain new advantages from the anonymous capabilities of the Internet and electronic commerce.

Such a system is necessary to protect consumers from con artists who would otherwise thrive in an anonymous world. The concept of confidentiality is not new and is, in effect, the one that the drafters of the constitution selected to limit the authority of law enforcement.

The founders rejected a system under which law enforcement could have unfettered access to the property of citizens, where they equally rejected a system where the property could be immune from scrutiny under any and all circumstances.

The framers of the constitution created a system under which law enforcement could have access to a person's property, such as his or her papers under appropriate judicial supervision by warrant or subpoena.

This same kind of balancing that would, an approach that protects both anonymity and accountability is also necessary in the area of electronic commerce.

At this point and time, it is very difficult to forecast how the issues that we've been talking about here today are going to be resolved. However, the outcome of these issues may very well determine whether electronic commerce will better protect consumers from fraud or will allow it to flourish like never before.

CHAIRMAN PITOFSKY: Thank you very much. I want to thank all of you for wonderful presentations on this issue. Once again we don't have a great deal of time for discussion.

But let me open it up briefly. I think many of you have hit upon the same themes as Toren just it, that without consumer confidence and security, these knew electronic money devices will simply not take off; history has demonstrated that in other contexts.

And the question is how we achieve that, whether we wait and let the market produce it or whether we need some kind of regulation. Miss Meier zeroed in on the point emphasizing I thought that without limited liability we'll be slower in developing these new devices, by which I take it you mean that consumers have to have confidence that if the card is lost or stolen we're talking about maybe $50 of exposure, $100 of exposure.

But if it's unlimited exposure they're going to be reluctant to use these new devices. Two questions. One, would that do it? Is that the critical regulatory requirement that's needed?

And then I would ask others, can we get there without

regulation, without statute? But first, is that the critical regulation that you think is necessary?

MS. MEIER: On the security question, I think that is the approach that's wise. Right now for credit cards we have $50 as the liability limit in the face of fraud against the consumer, unauthorized use of the credit card.

And that has worked well in protecting consumers. Not against fraud; we all know credit card fraud is a problem. But the consumer who faces it, financial losses are limited with that kind of ceiling.

With traditional debit cards, the Electronic Funds Transfer Act, which is also Regulation E, limits liability somewhat. But it is not as protective of consumers as the credit card rules are.

You may know that there has been some degree of request on the part of the financial services industry to ask for an exemption for stored value cards even from Regulation E.

We come at it totally opposite and say that we need to be looking at the adequacy of Regulation E with this new product.

CHAIRMAN PITOFSKY: How do the rest of you feel about this? Do we need an extension of the current regulations from credit cards to these other new forms of credit instruments?

MR. McENTEE: Mr. Chairman, I will be glad to try to answer that question. I think the issue that Michelle brought to the Task Force's attention, it's basically an off-line debit card. It's my understanding that debit cards do come under Regulation E today whether they're on-line debit cards or off-line debit cards.

So the liability limits that are in Regulation E that apply to consumers would apply for the types of transactions that Michelle described. But she's absolutely right. There is a difference in the liability limit under Regulation Z covering credit card transactions, which is $50.

Regulation E, it could be higher than $50 depending upon whether the consumer knew that the card was lost and the consumer did not notify the financial institution that the card was lost.

But under the problems that Michelle described, I believe it was not a card that was lost or stolen, someone got ahold of the number, basically the account number that was on the card.

So in that case the consumer's account would be, the liability would be limited to $50. Michelle is shaking her head no.

MS. MEIER: There are various patterns. And the one that was reported in the Times was actual loss of the card. And the thieves just used the card like a credit card at various retail outlets. But there have been instances where the number was pilfered and used to make telephone purchases.

MR. McENTEE: But again in all cases the consumer's liability would be limited under existing Regulation E. And virtually all the systems that all the people have talked about

today, either Regulation Z or Regulation E would apply. So consumers' liability is limited.

MS. MEIER: Yes. Actually when I looked at what was happening with the off-line debit card and realized that Reg. E applied, it gave me a whole new area of concern and provoked a lot of thought.

There is protection there theoretically, and it has worked well as long as institutions were using a pin, a secure system.

But I scratched my head and said, why isn't the institution's co-liability deterring the implementation of a system that is so unsecure?

And you have to look at the economics there. But apparently the judgment call at this point on the part of the private sector is that the fee income, the merchant fee income, which is quite high, is going to offset the liability losses that they'll be exposed to.

And in the meantime the consumer is out there exposed to more liability than ever before. And again the question is, is Regulation E creating the incentives that are protective enough?

CHAIRMAN PITOFSKY: Thank you. Other questions?

MR. SAFDAR: Yes, sir. I think it's necessary to respond to Mr. Toren's very critical and careful, veritable Sherman's march against anonymity.

I would hope that we could all appreciate the fact that there are important issues of anonymity here but we should restrict them to electronic payments since that is what the Task Force is about.

I understand that anonymity is not an all or nothing issue. In the marketplace are many, many different entities, many of whom do or do not have an expectation of anonymity.

When I go to the corner to buy anything, a jug of water, Poland Spring, whatever, and I expect some anonymity for the five dollars. And it's important to me as a consumer as I go into these new forms of transactions that I retain that because it's not as important to the shop keeper.

And instead of just assuming that anonymity is an all or nothing deal, as Mr. Toren would point us, a nothing in the future, may we at least consider teasing out, to use another phrase, some of the people in the marketplace to whom anonymity is not so important which allows us to respect some of the law enforcement goals.

CHAIRMAN PITOFSKY: Thank you.

Let me thank you all once again for an extremely useful session and we'll be sure to take your views into account.